



REC'D	FR99/583
WIPO	PCT
07 AVR. 1999	

# BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

**PRIORITY  
DOCUMENT**

SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

**COPIE OFFICIELLE**

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le **24 MARS 1999**

Pour le Directeur général de l'Institut  
national de la propriété industrielle  
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT  
NATIONAL DE  
LA PROPRIÉTÉ  
INDUSTRIELLE

SIEGE  
26 bis, rue de Saint Petersburg  
75800 PARIS Cédex 08  
Téléphone : 01 53 04 53 04  
Télécopie : 01 42 93 59 30



26 bis, rue de Saint Pétersbourg  
75800 Paris Cedex 08  
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

# BREVET D'INVENTION, CERTIFICAT D'UTILITE

Code de la propriété intellectuelle-Livre VI

**cerfa**  
N° 55 -1328

## REQUÊTE EN DÉLIVRANCE

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

DATE DE REMISE DES PIÈCES <b>20 MAR 1998</b>		1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE	
N° D'ENREGISTREMENT NATIONAL <b>98 03471 -</b>		<b>GEMPLUS S.C.A.</b> <b>hard NONNENMAYER</b> <b>Z I ATHELIA III</b> <b>Voie ANTIOPE</b> <b>13600 - LA CROTAT</b>	
DÉPARTEMENT DE DÉPÔT <b>75</b>			
DATE DE DÉPÔT <b>20 MARS 1998</b>			
2 DEMANDE Nature du titre de propriété industrielle			
<input checked="" type="checkbox"/> brevet d'invention <input type="checkbox"/> demande divisionnaire <input type="checkbox"/> demande initiale			
<input type="checkbox"/> certificat d'utilité <input type="checkbox"/> transformation d'une demande de brevet européen <input type="checkbox"/> brevet d'invention <input type="checkbox"/> certificat d'utilité n°			
Établissement du rapport de recherche <input checked="" type="checkbox"/> différé <input type="checkbox"/> immédiat			
Le demandeur, personne physique, requiert le paiement échelonné de la redevance <input type="checkbox"/> oui <input checked="" type="checkbox"/> non			
Titre de l'invention (200 caractères maximum)			
<b>DISPOSITIFS POUR MASQUER LES OPERATIONS EFFECTUEES DANS UNE CARTE A MICROPROCESSEUR.</b>			
3 DEMANDEUR (S) n° SIREN <b>7 49 7 1 1 2 0</b> code APE-NAF		Forme juridique	
Nom et prénoms (souligner le nom patronymique) ou dénomination		<b>Société en Commandite par Actions</b>	
<b>GEMPLUS</b>			
Nationalité (s) <b>Française</b>		Pays	
Adresse (s) complète (s)		<b>FRANCE</b>	
<b>Avenue du Pic de Bertagne</b> <b>Parc d'activités de la Plaine de Jouques</b> <b>13420 GEMENOS</b>			
4 INVENTEUR (S) Les inventeurs sont les demandeurs <input type="checkbox"/> oui <input checked="" type="checkbox"/> non Si la réponse est non, fournir une désignation séparée			
5 RÉDUCTION DU TAUX DES REDEVANCES <input type="checkbox"/> requise pour la 1ère fois <input type="checkbox"/> requise antérieurement au dépôt : joindre copie de la décision d'admission			
6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE			
pays d'origine      numéro      date de dépôt      nature de la demande			
7 DIVISIONS antérieures à la présente demande n°      date      n°      date			
8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (nom et qualité du signataire - n° d'inscription)		SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION      SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI	
<b>Paul BALLOT</b> <b>92-1009</b> <b>CABINET BALLOT SCHMIT</b>			

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

BA 540 4/1/1998 U



# BREVET D'INVENTION, CERTIFICAT D'UTILITE

## DÉSIGNATION DE L'INVENTEUR

(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

DIVISION ADMINISTRATIVE DES BREVETS

26bis, rue de Saint-Petersbourg

75800 Paris Cédex 08

Tél. : 01 52 04 53 04 - Télécopie : 01 42 93 59 30

SM/013939

N° D'ENREGISTREMENT NATIONAL

9803471

TITRE DE L'INVENTION :

**DISPOSITIFS POUR MASQUER LES OPERATIONS EFFECTUEES DANS UNE CARTE A MICROPROCESSEUR.**

LE(S) SOUSSIGNÉ(S)

**Cabinet BALLOT SCHMIT**  
**7, rue Le Sueur**  
**75116 PARIS**  
**FRANCE**

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

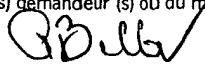
**NACCACHE David**  
**FEYT Nathalie**  
**BENOIT Olivier**

domicilié (s) au :

**Cabinet BALLOT SCHMIT**  
**7, rue Le Sueur**  
**75116 PARIS**  
**FRANCE**

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

  
**Paris, le 3 avril 1998**

**Paul BALLOT 92-1009**  
**Cabinet BALLOT SCHMIT**

**DOCUMENT COMPORTANT DES MODIFICATIONS**

[illegible]

Un changement apporté à la rédaction des revendications d'origine, sauf si celui-ci découle des dispositions de l'article R.612-36 du code de la Propriété Intellectuelle, est signalé par la mention «R.M.» (revendications modifiées).

DISPOSITIFS POUR MASQUER LES OPERATIONS EFFECTUEES DANS  
UNE CARTE A MICROPROCESSEUR

L'invention concerne les cartes à microprocesseur et, dans de telles cartes, différents dispositifs pour masquer les opérations effectuées dans la carte dans le but d'améliorer la sécurité contre les intrusions frauduleuses.

Les cartes à puces se divisent en plusieurs catégories, à savoir :

- les cartes à simple mémoire,
- les cartes à mémoire dite carte intelligente, et
- les cartes à microprocesseur.

Une carte à simple mémoire permet d'effectuer des opérations de lecture et d'écriture dans la zone de mémoire morte électriquement effaçable de façon libre. Une telle carte est d'un faible coût mais elle ne présente pas une sécurité suffisante de sorte qu'elle est de moins en moins utilisée.

Une carte à mémoire intelligente améliore notamment la sécurité des opérations de lecture/écriture en les autorisant seulement lorsque certaines conditions réalisées sous forme câblée sont remplies.

Une carte de la troisième catégorie contient un microprocesseur capable d'exécuter des programmes enregistrés dans une mémoire et d'effectuer ainsi des calculs avec des données secrètes inaccessibles au monde extérieur à la carte. Ainsi, une clé enregistrée dans la mémoire peut servir à valider une transaction électronique telle qu'un achat ou une ouverture de porte sans avoir à être manipulée à l'extérieur de la carte.

Malheureusement, certains microprocesseurs présentent des consommations de courant qui dépendent des calculs effectués à l'intérieur de la carte. Ainsi, un calcul cryptographique comprenant une arborescence de calcul qui dépend des chiffres de la clé utilisée aura différentes empreintes de consommation de courant selon la valeur de la clé utilisée. Il en résulte qu'un fraudeur pourrait corrélérer l'empreinte de consommation de courant de la clé utilisée et ainsi remonter à la valeur de la clé.

Pour empêcher cette corrélation, une contre-mesure courante consiste à programmer l'algorithme cryptographique d'une manière telle que quelle que soit la valeur de la clé, l'algorithme passera toujours les mêmes étapes de calcul.

De nombreux algorithmes dits "orientés octets" se prêtent bien à ce mode de programme mais d'autres posent quelques problèmes techniques qui ne sont surmontables qu'au prix de performances calculatoires moins optimales.

La présente invention a donc pour but de mettre en oeuvre dans les cartes à microprocesseur des dispositifs pour masquer les opérations effectuées tout en permettant au programmeur le libre-choix des règles de programmation, qu'elles soient du type "orientées octets" ou non.

Ce but est atteint en modifiant ou brouillant la consommation de la carte de manière que son empreinte soit indépendante des calculs effectués.

Cette modification ou ce brouillage de l'empreinte peut être obtenue en ajoutant dans la carte un dispositif qui modifie la consommation de courant.

Dans un premier exemple de réalisation, ce dispositif consomme de la puissance électrique de

manière irrégulière ou aléatoire qui s'ajoute à celle de la consommation normale.

Dans un deuxième exemple de réalisation, ce dispositif réalise une consommation moyenne en réalisant, par exemple, une intégration du courant consommé.

Dans un troisième exemple de réalisation, ce dispositif déclenche le circuit de programmation ou d'effacement de la mémoire du microprocesseur qui consomme de la puissance de manière chaotique, puissance qui masque la consommation due aux opérations effectuées par le microprocesseur pendant la programmation ou l'effacement de la mémoire.

D'autres caractéristiques et avantages de la présente invention effectueront à la lecture de la description suivante d'exemples particuliers de réalisation, ladite description étant faite en relation avec les dessins joints dans lesquels :

- la figure 1 est un schéma fonctionnel d'un premier exemple de réalisation de l'invention,
- la figure 2 est un schéma fonctionnel d'un deuxième exemple de réalisation de l'invention, et
- la figure 3 est un schéma fonctionnel d'un troisième exemple de réalisation de l'invention.

Sur les figures qui montrent chacune schématiquement différents moyens pour réaliser l'invention, la puce électronique 10 contenant le microprocesseur de la carte comprend une unité centrale 12 et au moins une mémoire 14, par exemple du type connu sous l'acronyme anglo-saxon EEPROM FOR ELECTRICALLY ERASABLE PROGRAMMABLE READ ONLY MEMORY. Cette puce électronique présente plusieurs bornes d'entrée et/ou de sortie  $16_1$  à  $16_8$  dont l'une d'entre elles référencée  $16_1$  est connectée à un circuit

d'alimentation électrique 18 de tension  $V_{CC}$  tandis que celle référencée 16<sub>5</sub> est connectée à la masse.

Le circuit d'alimentation 18 alimente les différents éléments de la puce électronique 10 avec un courant  $I_{out}$  et, notamment, la mémoire 14 et l'unité centrale 12. Ce courant  $I_{out}$  varie en fonction des opérations effectuées par l'unité centrale et la mémoire et reflètent donc les calculs cryptographiques, ce qui pourrait permettre d'en déterminer la clé.

Pour que ce courant  $I_{out}$  ne reflète plus les opérations effectuées, l'invention propose de le modifier par un dispositif 20 ou 30, disposé dans la puce 10 et connecté, par exemple, sur la borne d'entrée 16<sub>1</sub>.

L'invention propose de modifier le courant de deux manières différentes. Une première en faisant en sorte que le dispositif 20 (figure 1) consomme du courant de manière aléatoire ou tout au moins irrégulière, consommation supplémentaire aléatoire qui s'ajoutant à la consommation normale de courant  $I_{in}$  rend aléatoire la valeur  $I_{out}$ .

La deuxième manière consiste à moyenner la valeur de  $I_{in}$ , ce qui ne permet pas de détecter les variations de  $I_{in}$  dues aux opérations effectuées.

Dans le premier cas, le dispositif 20 peut être réalisé à l'aide de résistances 30, en fait des transistors, qui sont alimentées ou non selon les signaux aléatoires fournis par un générateur 28. Les courants circulant dans les résistances alimentées augmentent, modifiant la valeur du courant total et masquant le courant dû aux calculs cryptographiques.

Dans le deuxième cas, la moyenne du courant  $I_{in}$  est obtenue par un intégrateur qui "lisse" les variations du courant  $I_{in}$  de manière à les effacer.



Selon l'invention, plusieurs dispositifs 20 ou 30, référencés  $20_1$  et  $30_1$  peuvent être connectés à différents endroits de la puce électronique, par exemple, sur le conducteur d'alimentation de l'unité centrale (référence 22). En outre, ces dispositifs 20,  $20_1$ , 30 et  $30_1$  peuvent être connectés ou non selon que les opérations doivent être sécurisées ou non, les connexions s'effectueront sous la commande de signaux fournis par l'unité centrale 12 (traits discontinus).

10 L'invention propose une troisième manière de brouiller la valeur de  $I_{out}$  en effectuant des opérations à sécuriser, telles que des calculs cryptographiques, pendant certaines phases des opérations de programmation ou d'effacement de la  
15 mémoire 14, ces opérations étant sur la commande de l'unité centrale 12.

Cette troisième manière repose sur l'utilisation d'une mémoire 14 de type EEPROM qui a la capacité d'auto-écriture.

20 Dans un mode habituel de fonctionnement, le microprocesseur met en marche un circuit de programmation 24 de la mémoire 14 selon les étapes suivantes :

- 1 - mise en marche de la pompe de charge,
- 25 2 - présentation sur le bus de données de la dernière à écrire,
- 3 - présentation sur le bus d'adresse de l'adresse écriture,
- 4 - mise en marche de la programmation,
- 30 5 - attente d'un délai de programmation,
- 6 - arrêt de la programmation,
- 7 - arrêt de la pompe de charge.

La programmation d'une cellule EEPROM nécessitant d'injecter des charges électriques dans la cellule

programmée, les étapes 4, 5 et 6 s'accompagnent d'une sur-consommation de courant d'apparence chaotique qui dépend essentiellement de la valeur de  $V_{CC}$ , de l'adresse, de la valeur programmée et de la température du composant.

Afin de masquer l'empreinte de consommation de courant d'un calcul cryptographique par exemple, l'invention propose d'utiliser la consommation chaotique des étapes 4, 5 et 6 en réalisant le calcul cryptographique pendant l'étape 5 d'une durée de quelques millisecondes.

Pour ce faire, le calcul cryptographique s'effectue selon les étapes suivantes :

- 1 - mise en marche de la pompe de charge,
- 2 - présentation sur le bus de données d'une donnée aléatoire,
- 3 - présentation sur le bus d'adresse d'une adresse écriture,
- 4 - mise en marche de la programmation,
- 5 - effectuer le calcul cryptographique,
- 6 - arrêt de la programmation,
- 7 - arrêt de la pompe à charge.

Par ces étapes, l'empreinte de la consommation de courant due au calcul cryptographique de l'étape 5 est masquée par l'écriture de la donnée aléatoire dans une partie déterminée 26 de la mémoire EEPROM réservée à cette fonction.

Au lieu d'un calcul cryptographique, l'étape 5 peut consister en toute opération à sécuriser vis-à-vis de l'extérieur.

Par ailleurs, au lieu de faire ces opérations à sécuriser lors d'une écriture dans la mémoire 14, elles peuvent être faites lors d'un effacement de la mémoire 14.

## REVENDECATIONS

- 1 - Dispositif pour masquer les opérations effectuées par un composant destiné à être intégré à une carte à puce, caractérisé en ce qu'il comprend au moins un moyen (20, 30, 28, 26) pour modifier la consommation de courant dudit composant lors de la réalisation desdites opérations.
- 2 - Dispositif selon la revendication 1, caractérisé en ce que le moyen pour modifier la consommation de courant comprend au moins un circuit intégrateur (30) du courant du composant de manière à moyenner les variations de ce courant au cours du temps.
- 3 - Dispositif selon la revendication 1, caractérisé en ce que le moyen pour modifier la consommation de courant comprend au moins un générateur (28) de signaux aléatoires et une batterie de résistances (20) dont l'alimentation de chacune des résistances est commandée par les signaux aléatoires.
- 4 - Dispositif selon la revendication 1, caractérisé en ce qu'il comprend une pluralité de moyens (20, 20<sub>1</sub>, 30, 30<sub>1</sub>) pour modifier la consommation de courant.
- 5 - Dispositif selon la revendication 1, caractérisé en ce que le moyen pour modifier la consommation de courant du composant dans le cas d'une mémoire (14) du type EEPROM, consiste à effectuer simultanément:
  - une opération d'écriture ou d'effacement de la mémoire (14) dite de masquage, et
  - une opération du microprocesseur.
- 6 - Dispositif selon la revendication 5, caractérisé en ce que, pour mettre en oeuvre une opération d'écriture de masquage, la mémoire (14) comprend une partie (26) dédiée à l'enregistrement d'une donnée aléatoire.
- 7 - Dispositif selon l'une des revendications 1 à 5, caractérisé en ce que la mise en route de chacun des moyens de modification de la consommation de courant est commandée par le microprocesseur (12) de manière à être mis en route pour les seules opérations à sécuriser.
- 8 - Dispositif selon la revendication 5, caractérisé en ce que le microprocesseur (12) réalise au moins le calcul cryptographique selon les étapes suivantes:
  - mise en marche de la pompe de charge,
  - présentation sur le bus de données d'une donnée aléatoire,
  - présentation sur le bus d'adresse d'une adresse écriture,
  - mise en marche de la programmation,
  - effectuer le calcul cryptographique,
  - arrêt de la programmation,
  - arrêt de la pompe de charge,de manière à masquer l'empreinte de la consommation de courant occasionnée par ledit calcul cryptographique.

9 - Procédé pour masquer les opérations effectuées par un composant, caractérisé en ce qu'il comporte les étapes suivantes:

- mise en marche de la pompe de charge,
- présentation sur le bus de données d'une donnée aléatoire,
- présentation sur le bus d'adresse d'une adresse écriture,
- mise en marche de la programmation,
- effectuer le calcul cryptographique,
- arrêt de la programmation,
- arrêt de la pompe de charge.

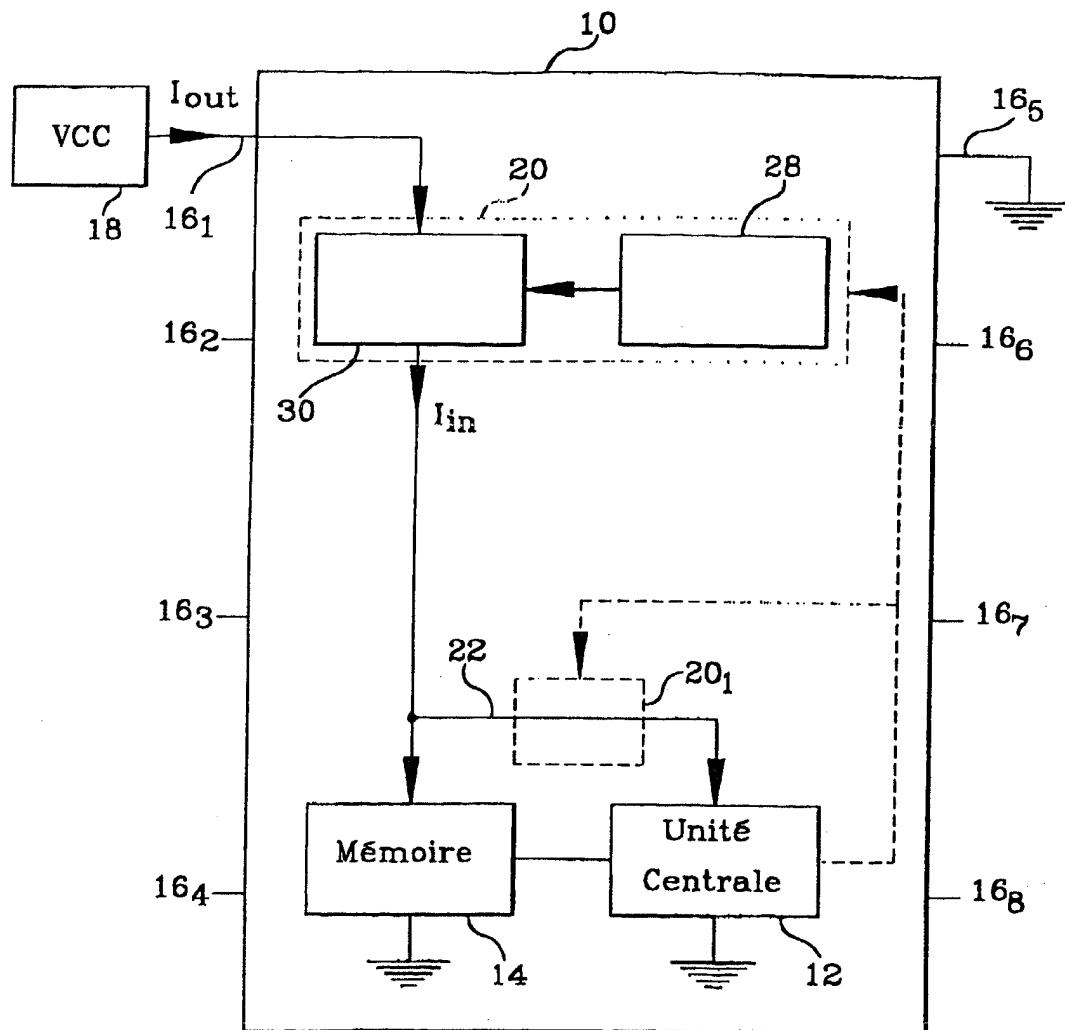
## REVENDICATIONS

1. Dispositif pour masquer les opérations effectuées par un composant destiné à être intégré à une carte à puce à microprocesseur, caractérisé en ce qu'il comprend au moins un moyen (20, 30, 28, 26) pour  
5 modifier la consommation de courant dudit composant lors de la réalisation desdites opérations.
2. Dispositif selon la revendication 1, caractérisé en ce que le moyen pour modifier la consommation de  
10 courant comprend au moins un circuit intégrateur (30) du courant du composant de manière à moyenner les variations de ce courant au cours du temps.
3. Dispositif selon la revendication 1, caractérisé en ce que le moyen pour modifier la consommation de  
15 courant comprend au moins un générateur (28) de signaux aléatoires et une batterie de résistances (20) dont l'alimentation de chacune des résistances est commandée par les signaux aléatoires.  
20
4. Dispositif selon la revendication 1, caractérisé en ce qu'il comprend une pluralité de moyens (20, 20<sub>1</sub>, 30, 30<sub>1</sub>) pour modifier la consommation de courant.
- 25 5. Dispositif selon la revendication 1, caractérisé en ce que le moyen pour modifier la consommation de courant du composant dans le cas d'une mémoire (14) du type EEPROM, associée à une unité centrale (12) du microprocesseur, comprend un moyen pour effectuer  
30 simultanément une opération d'écriture ou d'effacement

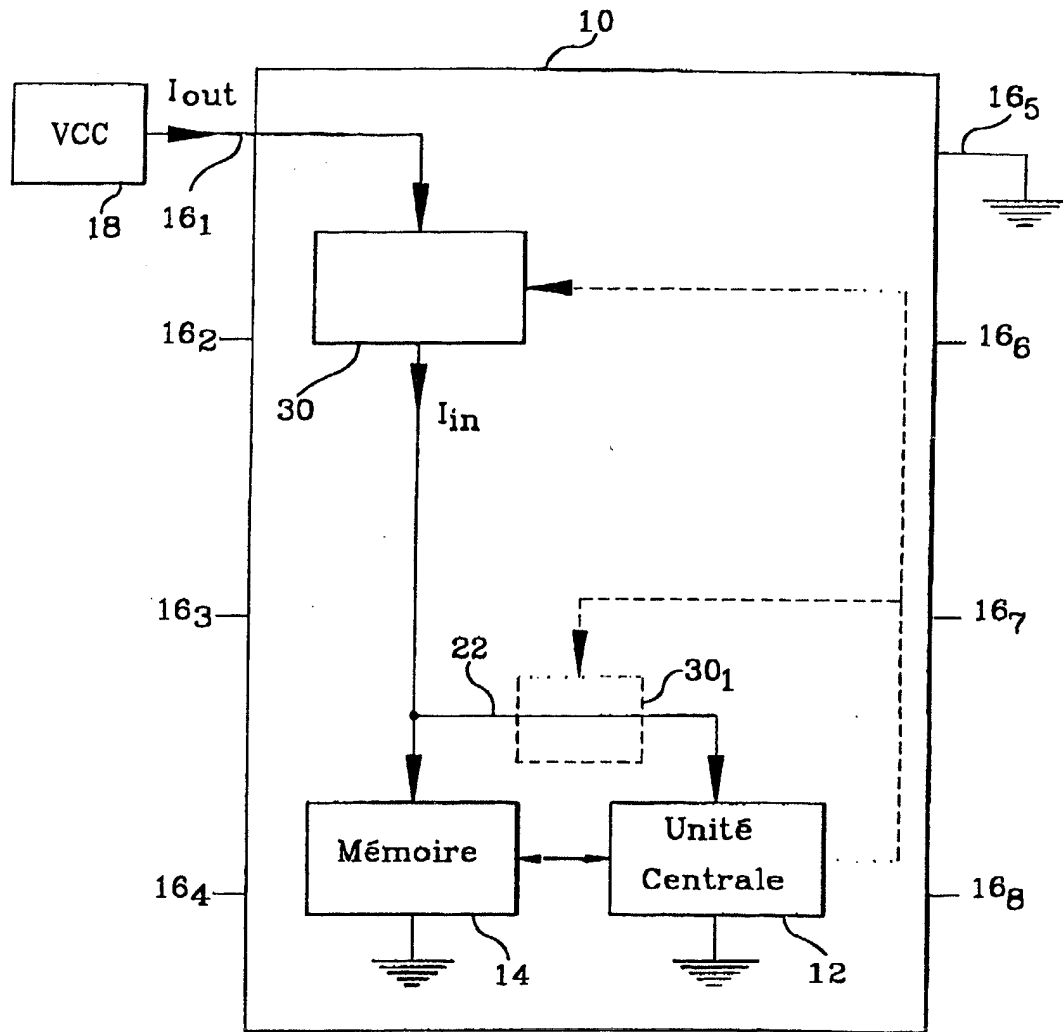
d'une mémoire (14) dite de masquage et une opération du microprocesseur.

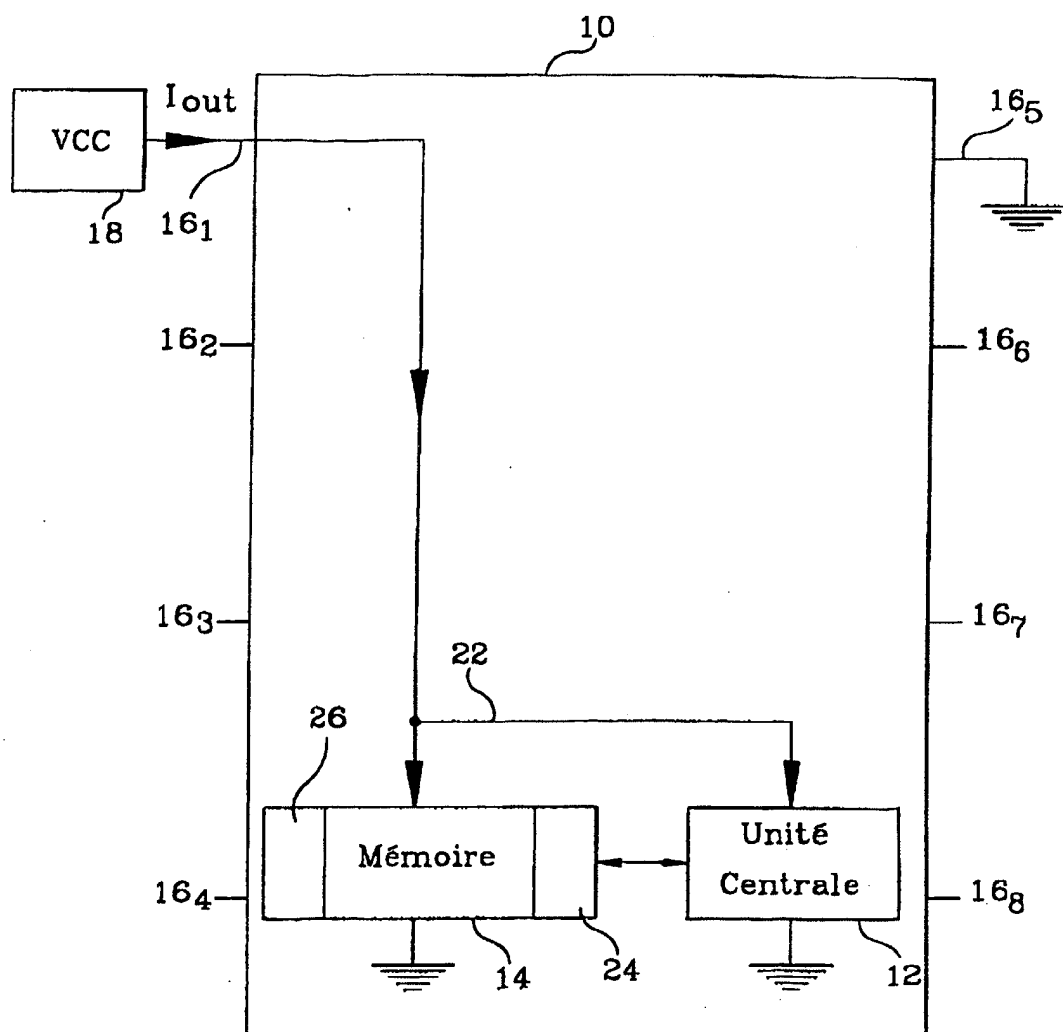
- 5 6. Dispositif selon la revendication 5, caractérisé en ce que, pour mettre en oeuvre une opération d'écriture ou d'effacement dite de masquage, la mémoire (14) comprend une partie (26) dédiée à l'enregistrement d'une donnée aléatoire.
- 10 7. Dispositif selon l'une des revendications 1 à 6, caractérisé en ce qu'il comprend, en outre, un moyen de mise en route de chacun des moyens de modification de la consommation de courant à chaque opération à sécuriser.
- 15 8. Procédé pour mettre en oeuvre le dispositif selon la revendication 5 ou 6, caractérisé en ce que, dans le cas d'un calcul cryptographique, il comprend les étapes suivantes consistant à :
- 20 - mettre en marche la pompe de charge,  
- présenter une donnée aléatoire sur le bus de données,  
- présenter une adresse d'écriture sur le bus d'adresses,  
- mettre en marche la programmation,
- 25 - effectuer le calcul cryptographique,  
- arrêter la programmation, et  
- arrêter la pompe de charge.
- 30 9. Procédé pour masquer les opérations effectuées par un composant, caractérisé en ce qu'il comporte les étapes suivantes :
- mise en marche de la pompe de charge,  
- présentation sur le bus de données d'une donnée aléatoire,

- présentation sur le bus d'adresses d'une adresse d'écriture,
- mise en marche de la programmation,
- réalisation du calcul cryptographique,
- 5 - arrêt de la programmation, et
- arrêt de la pompe de charge.

**FIG.1**



**FIG.2**

**FIG.3**

Smart-Card Based  
Access Control System with Improved Security

5           The present invention involves access control systems including an integrated circuit (IC) card, or "smart" card, for limiting access to information in signal processing applications. Systems such as pay-TV systems include access control sub-systems that limit access to certain programs or channels. Only  
10 users who are entitled (e.g., paid a fee) are permitted to view the programs. One approach to limiting access is to modify the signal by, for example, scrambling or encrypting the signal. Scrambling typically involves modifying the form of the signal using methods such as removing synchronization pulses. Encryption involves  
15 modifying a data component included in the signal according to a particular cryptographic algorithm. Only individuals who are entitled to access are given the "key" needed to descramble or decrypt the signal. The terms scrambling and descrambling as used below are intended to encompass access control techniques  
20 in general, including cryptography and scrambling.

          Access control systems may include an integrated circuit (IC) card, or "smart" card, feature. A smart card is a plastic card the size of a credit card that has a signal processing IC embedded in the plastic. A smart card is inserted into a card  
25 reader that couples signals to and from the IC in the card. International Standards Organization (ISO) standard 7816 establishes specifications for an IC card interface. In particular, ISO standard 7816-2 specifies that the electrical interface to the card will be via eight contacts positioned on the card surface as  
30 shown in Figure 2A. Six of the eight signals at the contact points are defined as VCC (supply voltage), RST (reset signal), CLK (clock signal), GND (ground), VPP (programming voltage for programming memory in the card IC), and I/O (serial data input/output). Two contacts are reserved for future use. The

assignment of the signals to the smart card contacts is shown in Figure 2B.

The IC in a smart card processes data such as security control information as part of an access control protocol. The IC  
5 includes a control microcomputer, such as the 6805 processor from Motorola Semiconductor, Austin, Texas, which includes ROM, EEPROM, and RAM memory. The processor performs various security control functions including entitlement management and generating the key for descrambling the scrambled data  
10 component of the signal.

Entitlement management involves modifying information stored in the card that specifies the card owner's entitlements (i.e. programs and services that a user is entitled to access). The processor adds and deletes entitlements in response  
15 to entitlement information in entitlement management messages (EMM) that are included in the input signal. EMM data typically indicates entitlement to a particular service, e.g. all programming on a particular channel, or to a particular program offered by a service, e.g., one movie on a particular channel. Because EMM  
20 relates to relatively long term entitlement, EMM typically occurs infrequently in a signal.

Once entitled to a service or program, descrambling of the service or program can occur only after generating a descrambling key. Key generation occurs in response to  
25 entitlement control messages (ECM) that are also included in the input signal. ECM provides initialization data for key generation routines that are executed by the processor. Each time a service provider changes the scrambling key, ECM data is included in the signal so that a system entitled to access can generate the  
30 corresponding new descrambling key. To aid in preventing unauthorized access to scrambled signals, the key is changed frequently, e.g., every two seconds. Thus, ECM data occurs frequently in the signal.

EMM and ECM data is transferred to the smart card for  
35 processing via the serial I/O terminal of the ISO standard 7816

interface. The serial I/O terminal is also used to transfer the generated key from the card to a descrambler unit in the video signal processing channel. The descrambler descrambles the data component of the input signal, e.g. video and audio data, using the key to produce a descrambled, or "plaintext", output signal. Descrambling involves reversing the effects of the scrambling process, e.g., re-inserting sync pulses or decrypting data using the inverse of the encryption algorithm. The descrambled signal is processed further by the signal processing channel to produce video and audio signals suitable for coupling to output devices such as a kinescope and a loudspeaker, respectively.

Including a descrambling function in the video signal processing channel involves adding descrambling hardware to the system. The hardware may be included in a consumer electronics (CE) device, such as a television receiver, or may be in a stand-alone decoder unit, such as a cable box. Including descrambling hardware in a CE device or separate decoder unit dedicates the device to a particular access control system. For example, the hardware may be appropriate for descrambling only a particular type of scrambling algorithm. If the service provider decides to change to a different access control system, e.g. due to security problems, replacing the descrambling hardware involves the expensive and difficult task of modifying CE devices and/or replacing decoder units.

In addition, transferring data between a smart card and the system using the smart card provides an opportunity for a hacker to attack the security system. Because the security control IC is embedded in the smart card, a hacker cannot access the IC directly as part of an attempt to "hack", i.e. defeat, the security algorithm. Attempting to de-laminate the smart card to access the IC will destroy the IC. However, a hacker can monitor a transfer of data between a smart card and other parts of the system. By monitoring a data transfer, a hacker might intercept key data being transferred to an external descrambler, thereby compromising the access control system. Similarly, a hacker can

monitor a transfer of entitlement data to and from the smart card. By detecting changes between entitlement data being input to a smart card and entitlement information being output from a smart card, a hacker might obtain information regarding the  
5 access control algorithm that is being used in the smart card.

The invention resides, in part, in recognition of the described problems and, in part, in providing a solution to the problems. In accordance with an aspect of the invention, a smart card processes first and second signal components of an input  
10 signal to produce corresponding first and second processed signals. The second processed signal is combined with the first signal component of the input signal to produce an output signal from the smart card.

In accordance with another aspect of the invention,  
15 the first signal component of the input signal is combined with the second processed signal to produce a predetermined timing relationship between the first signal component and the second processed component in the output signal.

In accordance with another aspect of the invention,  
20 the first signal component of the input signal is delayed before being combined with the second processed signal such that the output signal exhibits the predetermined timing relationship.

In accordance with another aspect of the invention, the predetermined timing relationship is substantially the same as  
25 a timing relationship that exists between the first and second signal components of the input signal.

In accordance with another aspect of the invention, the first signal component of the input signal is delayed through a first-in-first-out memory device included in the smart card prior  
30 to being combined with the second processed signal.

In accordance with another aspect of the invention, the first and second signal components of the input signal include scrambled information. The first and second processed signals include descrambled information corresponding to the scrambled

information in the first and second signal components of the input signal.

In accordance with another aspect of the invention, the first signal component of the input signal comprises scrambled entitlement data for a pay-for-access-service, such as a pay TV channel, and the second signal component of the input signal comprises scrambled data provided by the pay-for-access service provider, such as scrambled video or audio data.

The invention may be better understood by referring to the accompanying drawing in which:

Figure 1 shows, in block diagram form, a signal processing system including a smart card that provides both entitlement processing and descrambling;

Figure 2A shows the location of signal contacts on the surface of a smart card in accordance with ISO standard 7816-2;

Figure 2B shows the assignment of smart card interface signals to signal contacts shown in Figure 2A in accordance with ISO standard 7816-2;

Figure 3 shows a format that data included in a signal processed by the system shown in Figure 1 may exhibit;

Figure 4 shows, in block diagram form, an embodiment of signal processing functions included in a smart card suitable for use with the system shown in Figure 1;

Figures 5 through 8 illustrate signal routing through the smart card shown in Figure 4 during various modes of operation of the system shown in Figure 1;

An embodiment of a smart card access control system including the invention will be described in reference to an exemplary video signal processing system that is shown in block diagram form in Figure 1. The system shown in Figure 1 includes signal processing functions that may be found in various signal processing systems. A specific example is the DSS® direct-broadcast satellite television system developed by Thomson Consumer Electronics, Inc.

For a pay-TV service that involves a smart card based access control system, a user wishing to purchase the service contacts the service provider, pays a service-access fee and receives a smart card. A card is issued to a user with initial  
5 entitlement information stored in the card's EEPROM. Entitlement information may include data identifying the user and data specifying the scope of initial access entitlement (e.g., duration and/or specific programs the user has paid for). In addition, application-specific key generation software is stored in the card  
10 memory.

Entitlement information stored in the card can be modified by the service provider from a remote location using entitlement management messages (EMM) and entitlement control messages (ECM) that are inserted into portions of the signal. EMM  
15 includes information indicating subscription (long term access) and pay-per-view (single program access) services that the user has paid for. EMM may be directed to a particular smart card by including identification information in EMM data that corresponds to the identification information stored in the particular smart  
20 card. ECM includes data such as initialization data needed to generate descrambling keys. Thus, a signal for a particular program includes both a scrambled data component comprising video and audio data, and a control information component comprising EMM and ECM.

25 When the user wishes to access a pay-TV service, smart card 180 in Figure 1 is inserted into card reader 190. Card reader 190 couples signals between smart card 180 and a signal processing channel comprising units 100 through 170 in Figure 1. More specifically, card reader 190 connects to eight terminals that  
30 are located on the surface of smart card 180 as specified in ISO standard 7816-2 (see Figure 2). The connection established by card reader 190 creates interface 187 between smart card 180 and the signal processing channel. In accordance with an aspect of the invention described further below, the eight signals in  
35 interface 187 include signals 184, a high speed data input/output



(I/O) port for smart card 180, and signals 182, a subset of the ISO standard IC card interface signals.

The desired program or service is selected by tuning the receiver to the appropriate channel using tuner 100. Tuner 100 is controlled by microcontroller 160 in response to user inputs. For example, microcontroller 160 may receive channel selection signals from a remote control (not shown in Figure 1) activated by a user. In response to the channel selection signals, microcontroller 160 generates control signals causing tuner 100 to tune the selected channel.

The output of tuner 100 is coupled to forward error corrector (FEC) 110. FEC 110 monitors error control information, such as parity bits in the tuned signal, to detect errors and, depending on the error control protocol, to correct errors. Microcontroller 160 is coupled to FEC 110 to monitor the occurrence of errors in the signal and control the processing of errors. FEC 110 also performs an analog-to-digital conversion (ADC) function to convert the analog output of tuner 100 to a digital signal at the output of FEC 110.

Transport unit 120 processes the signal from FEC 110 to detect and separate various types of data in the tuned signal. The data in the signal may be arranged in various formats. Figure 3 shows an exemplary data format that serves as the basis for the following description. The signal depicted in Figure 3 comprises a stream of data organized in packets of data bytes, i.e. "packetized" data. Each packet is associated with a particular type, or sub-stream, of information in the tuned channel's data stream. For example, the signal includes packets of program-guide information, control information (e.g., ECM or EMM), video information, and audio information. The sub-stream that a particular packet is associated with is defined by data included in a header portion of each packet. A payload portion of each packet includes the packet data. The exemplary data format shown in Figure 3 includes two bytes (16 bits) of data in the header and 186 bytes of data in the payload.

The first twelve bits of the header in each packet are program identification (PID) data bits. PID data identifies the data substream that the payload data is associated with. An example of the information provided by PID data follows:

5

TABLE 1

<u>PID Value</u>	<u>Payload contents</u>
1	program-guide information
10 4	EMM
10 10	video data for channel 101
11 11	audio data for channel 101.

Other PID values identify video and audio data for other channels.

15

As part of the tuning process, microcontroller 160 refers to a PID "map" stored in the microcontroller's memory to determine the PID values associated with the tuned channel. The appropriate PID values are loaded into PID registers in transport unit 120. For example, when channel 101 is selected,

20

microcontroller 160 accesses the stored PID map, determines that video data and audio data for channel 101 are associated with PID values of 10 and 11, respectively, and loads the values 10 and 11 into respective video and audio PID registers in transport unit 120. The PID data in incoming packets is compared to the PID

25

values stored in the PID registers to determine the content of the payload of each packet. Microcontroller 160 can update the PID map data in response to PID-to-channel correspondence information in "program guide" packets (PID value of 1).

The last four bits of the header portion of each packet further define the payload contents as follows:

TABLE 2

5	<u>Header bit</u>	<u>Designation</u>	<u>Function</u>
	13	ECM flag	indicates if payload is ECM
	14	-	reserved
10	15	ENC flag	indicates if payload is encrypted
	16	Key flag	indicates whether payload key is key A or key B.

- 15 The ECM flag being active, e.g., at logic 1, indicates that the payload includes ECM data such as initialization data for key generation. The ENC flag being active indicates that the payload is encrypted and, therefore, must be descrambled. The key flag determines which one of two keys, key A or key B, should be used
- 20 for descrambling the payload (e.g., logic 0 indicates key A, logic 1 indicates key B). Use of the key flag is described below in regard to Figure 7.

- Transport unit 120 in Figure 1 extracts and processes the header data in response to a packet clock signal shown in
- 25 Figure 3. The packet clock signal is generated and synchronized to the data stream by FEC 110. Each transition of the packet clock signal indicates the beginning of a packet. Transport unit 120 processes the 16 bits of header data following each packet clock signal transition to determine the destination for the packet
- 30 payload. For example, transport unit 120 transfers payloads containing EMM (PID value of 4) and ECM to security controller 183 in smart card 180 via microcontroller 160. Video and audio data are directed to demux/descrambler 130 for descrambling and demultiplexing into video and audio signals. Program guide

data (PID value of 1) is directed to microcontroller 160 for PID map updating.

Security controller 183 processes EMM and ECM data to provide access control functions including entitlement management and key generation. Security controller 183 is included in integrated circuit (IC) 181 and comprises a microprocessor such as the 6805 processor from Motorola. Entitlement management involves processing EMM data to determine how and when entitlement information stored in IC 181 is to be updated, i.e. adding and deleting entitlements. ECM data provides initial values needed for security controller 183 to generate descrambling keys. After being generated by security controller 183, a key is transferred via microcontroller 160 to descrambler 130 where the scrambled data component of the input signal, e.g., the video and audio program data, from the tuned channel is descrambled. In accordance with principles of the invention that are described further below, the descrambling function may also be provided by descrambler 185 included in IC 181.

Descrambled video and audio data is decompressed in video decompressor 140 and audio decompressor 145, respectively. Program data is compressed at the program source using any one of a variety of known data compression algorithms. Decompressors 140 and 145 reverse the effects of the compression algorithm.

The outputs of video and audio decompressors 140 and 145 are coupled to respective video and audio signal processors 150 and 155. Audio signal processor 155 may include functions such as stereo signal generation and digital to analog conversion for converting the digital output signal from decompressor 145 to an analog audio output signal AOUT from processor 155 that can be coupled to a loudspeaker (not shown in Figure 1). Video signal processor 150 also includes digital to analog conversion capability to convert the digital output of decompressor 140 to an analog video output signal VOUT that is

suitable for display on a display device such as a kinescope. Video processor 150 also provides signal switching necessary to include an on-screen display (OSD) signal, produced by OSD processor 170, in signal VOUT. The OSD signal represents, for example, graphics information such as a channel number display that is to be included in the displayed image. Video switches in video processor 150 multiplex the OSD signal into signal VOUT as required to produce the desired display. The operation of OSD processor 170 is controlled by microcontroller 160.

Returning to the access control features of the system shown in Figure 1, the features and function of smart card 180 may be better understood by referring to the block diagram of smart card IC 181 that is shown in Figure 4. Reference numerals in Figure 4 that are the same as in Figure 1 indicate the same or similar features. In Figure 4, integrated circuit (IC) 181 includes security controller 183 comprising a central processing unit (CPU) 421, RAM 426, ROM 425, EEPROM 423 and serial I/O unit 424. CPU 421 is a processor such as the 6805 from Motorola. Key generation and entitlement management software is stored in ROM 425 and EEPROM 423.

Data specifying current entitlements is also stored in EEPROM 423 and is modified in response to information in entitlement management messages (EMM) in the received signal. When an EMM packet is detected by transport processor 120 in Figure 1 (packet PID value of 4), microcontroller 160 in Figure 1 transfers the packet payload to security controller 183 via serial I/O unit 424. CPU 421 transfers the EMM data in the payload to RAM 426. CPU 421 processes the EMM data and modifies entitlement data stored in EEPROM 423 accordingly.

Packet payloads that include entitlement control messages (ECM), as indicated by the ECM flag in the packet header being active, are transferred from transport unit 120 to security controller 183 via microcontroller 160 and serial I/O unit 424. Any type of packet, e.g., EMM, video, or audio, may include ECM. ECM data is used for generating the descrambling key for a

particular type of data. For example, ECM data in an EMM packet is used to generate an EMM descrambling key. When transferred to security controller 183, ECM data is stored in RAM 426 until processed by CPU 421. Key generation software stored in EEPROM 423 and ROM 425 is executed by CPU 421 using the ECM data in RAM 426 to generate a particular key. The ECM data provides information such as initial values required by the key generation algorithms. The resulting key is stored in RAM 426 until transferred by CPU 421 to descrambler 130 via serial I/O unit 324 and microcontroller 160.

EMM and ECM data may be encrypted as indicated by encryption flag ENC in the packet header being active. Encrypted data is transferred from transport unit 120 to descrambler 130 for descrambling before being transferred to security controller 183 for entitlement management or key generation processing.

The features and operation of IC 181 that have been described are typical of known smart card systems. As stated above, however, using a descrambling unit external to a smart card, such as descrambler 130, substantially degrades system security and makes changing descrambling hardware undesirable. The arrangement shown in Figures 1 and 4 includes features that significantly improve security in comparison to known smart card systems. In particular, IC 181 of smart card 180 includes descrambler unit 185 and high data rate synchronous interface 184 comprising separate serial data in and serial data out lines. The combination of descrambler 185 and interface 184 makes it possible for all access control processing to occur within smart card 180.

In Figure 1, card reader 190 couples both ISO standard interface signals 165 from microcontroller 160 and high speed interface signals 125 from transport unit 120 to smart card 180 via portions of smart card interface 187 that are labeled 182 and 184, respectively. Figure 4 shows the signals included in interface 187. ISO standard signals 182 comprise power, ground, reset, and serial I/O in Figure 4 (correspond to VCC, GND, RST, and I/O in

Figure 2B). High speed interface signals 184 comprise high speed data-in and data-out signals, a packet clock signal, and a high frequency (e.g. 50 MHz) clock signal. ISO standard signal VPP (programming voltage) is replaced by the packet clock signal  
5 allowing interface 187, including both high and low speed interfaces, to be implemented using the ISO standard configuration of eight contacts that is shown in Figure 2A.

Eliminating signal VPP does not preclude the system shown in Figure 1 from operating with existing ISO standard  
10 smart cards that do not include descrambler 185 and high speed data interface 184. Existing smart cards typically include EEPROM circuits that do not require a separate programming voltage. A "charge pump" feature generates the required programming  
15 required. Thus, the VPP signal as specified by the ISO standard is an "unused" terminal for most existing ISO standard smart cards. Use of the system with existing smart cards does require modifying the operation of the system such that high speed interface 184 and descrambler 185 are not used. The required  
20 modification can be achieved by changing only the control software for controller 160.

Descrambler 185 operates at a high data rate in response to the high frequency clock signal while security controller 183 requires a lower frequency clock signal. Divider  
25 422 in IC 181 divides the 50 MHz clock signal to produce a lower frequency clock signal suitable for security controller 183. Thus, the single high frequency clock signal serves as a timing signal for controlling the operation of both security controller 183 and descrambler 185. Using divider 422 avoids dedicating two of the  
30 eight smart card interface signals to separate high and low frequency clock signals.

Descrambler 185 includes transport decode unit 472, PID & ECM filter unit 474 and EMM address filter unit 476 for providing functions similar to the above-described functions of  
35 transport unit 120 in Figure 1. The high speed data-in and data-

out signals of interface 187 couple the high speed data stream of the input signal between transport unit 120 and descrambler 185. Including functions of transport unit 120 within smart card 180 enables smart card 180 to process incoming data packets at the  
5 high data rate of the input signal. Both the data-in and packet clock signals are coupled to unit 472.

In response to each transition in the packet clock signal, unit 472 processes the 16 bits of header data. The first 12 bits of the header are program identification (PID) data that are  
10 directed to PID & ECM filter unit 474. Unit 474 compares the packet's PID data to PID values stored in unit 474 for each type of packet included in the tuned channel. Similarly to the above-described operation of transport unit 120 (see Table 1 above and associated description), PID comparison in unit 474 determines  
15 what type of data the payload contains, e.g., program guide, EMM, video, or audio. PID values identifying packet types in the currently tuned signal are stored in registers in unit 474. The registers are loaded as part of the above-described tuning process for the system in Figure 1. More specifically, microcontroller 160  
20 accesses a stored PID "map" as described above and transfers PID values associated with the currently tuned channel to registers in unit 474 via signals 182 and security controller 183 in smart card 180. Transfer of data between security controller 183 and functions of descrambler 185, such as unit 474, occurs via a data  
25 bus internal to IC 181 that is not shown in Figure 4.

How the payload data is processed by smart card 180 is determined both by the results of PID comparison in unit 474 and by the contents of bits 13 to 16 of the packet header extracted by unit 472. Using the example above relating to  
30 channel 101 (see Table 1), PID data identifies: program guide data (PID = 1) that microcontroller 160 processes to update the PID map, EMM data (PID = 4) that security controller 183 processes to modify entitlements, video data (PID = 10) and audio data (PID = 11). Bits 13 through 16 of the header control security-related  
35 operations (see Table 2 above and the associated description) in



15

smart card 180. If bit 13 (ECM flag) is active, the payload includes ECM data that requires key generation processing by security controller 183. If bit 15 (ENC flag) is active, the payload is encrypted and is descrambled in descrambling unit 478 within descrambler 185. Bit 16 determines whether key A or key B will be used in unit 478 for descrambling.

The encryption status bit ENC determines how payload data will be processed by descrambling unit 478. Payload data that is not encrypted passes unchanged from the high speed data-in terminal of smart card 180 through descrambling unit 478 to the high speed data-out terminal. Encrypted data is descrambled at the data rate by unit 478. Descrambled video and audio data is passed to the high speed data-out terminal of smart card 180. In each descrambled audio or video packet, the ENC bit in the packet header is set to logic 0 indicating that the packet is "clear", i.e. descrambled.

To ensure that unauthorized users do not access descrambled entitlement or key related data, descrambled EMM or ECM data is not passed out of smart card 180 via the high speed data out terminal. One approach is for the smart card to simply remove the EMM or ECM data component from the data stream at the output of the smart card. However, by monitoring changes that occur to data in the data stream between the data input and output of smart card 180, a hacker could obtain useful information regarding the processing that is occurring in smart card 180. For example, a hacker could assume that information removed from the data stream by the smart card pertains to the service associated with the smart card.

This problem is overcome by passing the original scrambled EMM or ECM control information component, with the ENC bit set to logic 1, through smart card 180 from the high speed data-in terminal to the high speed data-out terminal. More specifically, a first signal component of the input signal, such as scrambled ECM or EMM control information, is processed, e.g., descrambled, by descrambler 478 to produce a first processed

signal such as descrambled data needed for key generation. Information such as key information in the first processed signal is used by descrambler 478 to process a second component of the input signal to produce a second processed signal representing, for example, descrambled video or audio data. The first signal component of the input signal is combined with the second processed signal to produce the output data stream from smart card 180. Thus, for example, scrambled entitlement information in the input signal may be descrambled and used by smart card 180, but corresponding data at the output is unchanged, thereby reducing the information that can be obtained by a hacker monitoring the data stream.

To further obscure the nature of processing occurring in smart card 180, the original component of the input signal is delayed before being re-inserted into the output data stream. The delay ensures that the timing relationship between scrambled control information, such as EMM and/or ECM, and descrambled data, such as video and/or audio data, in the data output signal of smart card 180 is substantially the same as the timing relationship between scrambled control information and scrambled data in the data input signal of smart card 180. As a result, it is more difficult for a hacker to determine characteristics of smart card 180 such as the internal descrambling delay by monitoring the data stream.

Original scrambled data is delayed and re-inserted in the data stream via first-in-first-out (FIFO) memory 477 and router 479 in Figure 4. The input data signal to FIFO 477 is the signal at the data input of descrambler 478. The delay through FIFO 477 can be adjusted by control processor 183 to provide a delay through FIFO 477 that corresponds to the particular descrambling algorithm being executed in descrambler 478. For example, the delay through FIFO 477 can be increased or decreased by storing more or less data, respectively, in the FIFO before beginning to read data from the FIFO. Router 479 combines delayed data from FIFO 477 with descrambled data

from descrambler 478 under control of control processor 183 to produce the data output signal from smart card 180. Router 479 may comprise a multiplexer for selectively coupling either the FIFO output or the descrambler output to the data output of smart card 180 in response to a control signal provided by control processor 183.

EMM and ECM data that is descrambled in descrambling unit 478 is stored temporarily in RAM 426 in security controller 183 until processed by security controller 183 for entitlement management and key generation. Transport unit 120 in Figure 1 receives the data (either unchanged or descrambled) from the high speed data-out terminal of smart card 180. The PID value of each packet is checked and the payload is transferred to the appropriate function in Figure 1 for further processing (e.g., microcontroller 160 or decompressors 140 and 145).

The operation of smart card 180 is controlled by commands from microcontroller 160 in Figure 1 that are communicated to smart card 180 via the ISO standard serial interface. In effect, microcontroller 160 is the master processor and security controller 183 is the slave processor. For example, microcontroller 160 transfers PID information to smart card 180 and directs the card to descramble the data in the corresponding data streams. Security controller 183 responds by checking entitlements and configuring smart card 180 for the appropriate type of data processing such as entitlement processing, key generation or descrambling. In addition, microcontroller 160 requests status information such as whether descrambling is in progress. Commands are communicated to security controller 183 in smart card 180 via the serial I/O terminal. Any response required by the command is returned to microcontroller 160 via the serial I/O terminal. Thus, the serial I/O signal serves as a control signal between the system and smart card 180 while the high-speed data interface provides high-speed input and output data signals between the card and the system.

Serial communications between microcontroller 160 and smart card 180 occur according to a protocol provided for in ISO standard 7816-3. A smart card notifies the system of the particular protocol that will be used by sending a protocol type number T to the system. More specifically, when a card is inserted into the card reader, the card reader applies power to the card and resets the card by activating the reset signal. The card responds to the reset signal with an "answer to reset" data sequence specified in ISO standard 7816-3 §6. The answer to reset includes an interface byte TDi. The four least significant of byte TDi define the protocol type number T (see ISO standard 7816-3 §6.1.4.3).

The protocol type for the system shown in Figure 1 is type T=5. A type 5 protocol is classified as "reserved", i.e. currently undefined, in the ISO standard. For the system in Figure 1, protocol type 5 is identical to protocol type 0 (an asynchronous half-duplex protocol defined in ISO 7816-3 §8) except for the manner in which the baud rate for serial I/O is determined. Serial I/O at the card interface occurs at a rate determined according to Table 6 in ISO standard 7816-3. The baud rate calculation is based on the rate at which security controller 183 is clocked. For existing smart cards, the clock frequency for security controller 183 is equal to the clock frequency  $f_s$  at the card's clock pin. As shown in Figure 4, smart card 180 includes divider 422 for dividing the rate of the high speed input clock  $F_{in}$  by a factor N, i.e.  $F_{in}/N$ , to establish the clock rate for security controller 183. Thus, for a type 5 protocol, Table 6 of ISO standard 7816-3 is modified by defining  $f_s = F_{in}/N$ .

As in the case of a type 0 protocol, all commands for a type 5 protocol are initiated by microcontroller 160. A command begins with a five byte header including a one-byte instruction class designation (CLA), a one-byte instruction (INS), a two-byte parameter (P1,P2) such as an address, and a one-byte number (P3) defining the number of data bytes that are part of the command and follow the header. For the system in Figure 1,

parameter P1,P2 is not needed and, therefore, these bytes are "don't cares". Thus, commands take the form:

CLA | INS | - | - | P3 | data (P3 bytes).

5

Commands recognized by smart card 160 include a status command and a PID transfer command. Smart card 160 responds to a status command from microcontroller 160 by providing the processing status of the card, e.g. whether the card has completed key generation or whether the card is descrambling data. Using a PID transfer command, microcontroller 160 transfers PID numbers associated with the tuned channel. Other commands such as commands for transferring EMM and ECM data, key related commands, and "purchase offer" commands are possible and will be explained below.

The operation of smart card 180, and in particular descrambler 185, will now be described in more detail in reference to Figures 5 through 8. When a new channel is tuned, microcontroller 160 transfers PID values for the new channel from the PID map to smart card 180 as shown in Figure 5. The PID data transfer occurs using a PID transfer command including N PID values, where N is specified in byte P3 of the command header. The command and PID values are communicated to the card via the serial data terminal of smart card 180 and serial input/output unit 424. CPU 421 receives the PID data and directs the data to the appropriate PID register in registers 474 in descrambler 185.

Before a signal can be descrambled, a user must be entitled to access and the correct key must be loaded into descrambler 185. After transfer of the PID data to smart card 180, security controller 183 compares the PID values to entitlement data stored in EEPROM 423 to see if the user is entitled to access the tuned channel. Assuming the user is entitled, the next step is key generation. Key generation involves

processing ECM data. Thus, ECM must be received and processed to produce the key before audio and video data can be descrambled. ECM data is encrypted to reduce the likelihood of unauthorized key generation. A card is issued with a key for  
5 descrambling ECM stored in the card in EEPROM 423. As illustrated in Figure 6, the ECM key is transferred by CPU 421 from EEPROM 423 to ECM key registers in descrambling unit 478.

If the user is not entitled to access the tuned channel, entitlements must be received before key generation and  
10 descrambling can occur. Entitlements can be received via EMM. An "address" identifying a particular smart card is stored in EMM address unit 476 of the card when the card is issued. By including address information in EMM, a service provider can direct EMM to a particular card. The smart card compares the address  
15 information in EMM with the card address stored in unit 476 to detect EMM information directed to the card. If a user is not entitled, security controller 183 configures the card for EMM processing as shown in Figure 6 in case EMM data is received.

As in the case of the ECM key, a card is issued with an  
20 EMM key stored in the card in EEPROM 423. In Figure 6, the EMM key is transferred from EEPROM 423 to EMM key registers in descrambling unit 478 by CPU 421. Scrambled EMM data from transport unit 120 in Figure 1 is input to the card via the high speed data-in port. After checking the EMM address in unit 476,  
25 EMM data intended for the card is decrypted in descrambling unit 478. Decrypted EMM data is temporarily stored in RAM 426 and processed by CPU 421 to update entitlement data stored in EEPROM 423.

After the PID values are loaded, entitlements exist,  
30 and the ECM key is in place in descrambler 185, the card is ready to descramble ECM data and generate the audio and video keys. In Figure 7, ECM data in the signal is received by smart card 180 via the high speed data-in terminal and detected by transport decode unit 472. The ECM data is directed to descrambler 478  
35 where the previously loaded ECM key is used to decrypt the ECM

data. The decrypted ECM data is transferred from descrambler 478 to RAM 424. When decrypted ECM data is available, CPU 421 executes key generation algorithms stored in EEPROM 423 and ROM 425 using the decrypted ECM data in RAM 424 to generate the video and audio keys. The generated keys are transferred to the appropriate video and audio key registers in descrambler 478.

As shown in Figure 7, descrambler 478 includes two key registers for video, video keys A and B, and two key registers for audio, audio keys A and B. Whether key A or B will be used to descramble a particular packet is determined by the key flag bit in the packet header (see Table 2 above). The "multi-key" feature is used to permit a new key to be generated while an existing key is being used to descramble data. Processing ECM data in security controller 183 to generate a new key and transferring the new key to a key register in descrambler 478 requires a significant number of instruction cycles in CPU 421. If descrambling was halted during the generation and transfer of a new key, the processing delay would require someone viewing a program to watch a scrambled image until the new key was in place in descrambler 478. Having key registers A and B permits data to be decrypted using a key in one key register, e.g., key register A, while a new key is being generated and loaded into the second key register, e.g., key register B. After initiating key generation by transmitting ECM data, a service provider waits for a time period sufficient to ensure that new key B is generated and in descrambler 478 before encrypting packets using key B. The key flag notifies descrambler 185 when to begin using the new key.

After the operations shown in Figures 5, 6, and 7, descrambler 478 has been initialized with all key information needed to process encrypted data in the tuned channel, including EMM, ECM, video and audio data. Figure 8 shows the signal flow for data processing. Encrypted data enters smart card 180 via the high speed serial data input terminal. The data is decrypted in descrambler 478 using the previously loaded keys. For example, if transport unit 472 determines from the header of an incoming

packet that the payload data is video data associated with video key A, the packet payload is decrypted in descrambler 478 using video key A. The decrypted data is output directly from smart card 180 via the high speed serial data output terminal. Note that data processing in Figure 8 does not require interaction between descrambling unit 185 and security control unit 183 allowing descrambler 478 to process data at the high data rate of the input signal.

Key generation in security controller 183 combined with the descrambling features of descrambling unit 478 provides complete capability in smart card 180 for processing signals encrypted using a variety of algorithms including the data encryption standard (DES) algorithm and Rivest-Shamir-Adleman (RSA) algorithms. By providing all access control related processing within smart card 180, security related data such as key data does not have to be transferred out of smart card 180. As a result, security is improved significantly in comparison to systems using a descrambler external to the smart card.

Although the use of descrambler 185 internal to smart card 180 is advantageous, an external descrambler such as descrambler 130 in Figure 1 may also be used. An external descrambler may be desirable for compatibility of the described smart card with existing pay-TV systems that generate the key in smart card 180 and transfer the key to descrambler 130. Alternatively, using both descrambler 185 and descrambler 130 may be desirable. For example, security can be improved by encrypting a signal twice using two different keys. A twice-encrypted signal could be decrypted using the system shown in Figure 1 by: decrypting the signal once in descrambler 185 using the first key, transferring the partially decoded data to descrambler 130, and decrypting the signal a second time in descrambler 130 using the second key. The second key would be generated in smart card 180 and transferred to descrambler 130.

For applications involving descrambler 130 (i.e. applications in which key data is transferred out of smart card



180), commands are provided for transferring the key data via the serial I/O interface between controller 160 and smart card 180. For example, microcontroller 160 sends ECM data to the card in one command and requests the status of key generation with a status command. When the status data indicates that key generation is complete, another command requests the key data and the card responds by sending the key data to controller 160. Subsequently, the key is transferred to descrambler 130.

Various modifications of the described embodiments are possible. For example, it will be readily apparent to one skilled in the art that the invention is applicable to signals and systems other than those described. For example, video systems and video signal protocols other than that depicted in Figure 3 include the above-mentioned DSS® satellite system and high-definition television (HDTV). The described type of access control system is also applicable to signal processing systems such as cellular telephone systems in which processing entitlements may involve determining whether a user is entitled to access a cellular telephone system and, if so, processing a scrambled cellular telephone signal.

Applications such as a cellular telephone system involve generating an outgoing signal in addition to processing an incoming signal. Generating an outgoing signal requires encryption. The described smart card can encrypt data if appropriate encryption software is stored in EEPROM and ROM in smart card 180. Thus, the invention is applicable to signal source applications such as telephone systems or "head-end" applications in cable TV systems. These and other modifications are intended to be within the scope of the following claims.

Claims

1. A smart card comprising:  
a first terminal for receiving an input signal including  
5 first and second signal components;  
a second terminal for providing an output signal;  
means for processing said first signal component for  
producing a first processed signal, and being responsive to said  
first processed signal for processing said second scrambled  
10 component for producing a second processed signal; and  
means for combining said first signal component of  
said input signal and said second processed signal to produce said  
output signal.
- 15 2. The smart card of claim 1 wherein  
said means for combining said first signal component  
of said input signal and said second processed signal producing a  
predetermined timing relationship between said first signal  
component and said second processed signal in said output signal.
- 20 3. The smart card of claim 2 wherein said means  
for combining said first signal component of said input signal and  
said second processed signal comprising:  
means for delaying said first signal component to  
25 produce a delayed signal exhibiting substantially said  
predetermined timing relationship with respect to said second  
processed signal; and  
means for combining said delayed signal and said  
second processed signal to produce said output signal.

30

35

4. The smart card of claim 3 wherein  
said input signal exhibiting an input timing  
relationship between said first signal component and said second  
signal component; and

5 said predetermined timing relationship being  
substantially the same as said input timing relationship.

5. The smart card of claim 4 wherein said first and  
second signal components of said input signal comprise respective  
10 first and second scrambled signal components and said first and  
second processed signals comprise respective first and second  
descrambled signals.

6. The smart card of claim 5 wherein said means  
15 for delaying said first signal component of said input signal  
comprises a first-in-first-out memory device.

7. The smart card of claim 6 further comprising  
means responsive to said first descrambled signal for producing  
20 control information; said means for producing said first and  
second descrambled signals being responsive to said control  
information for producing said second descrambled signal.

8. The smart card of claim 7 wherein  
25 said means for producing said first and second  
descrambled signals, said means for producing said control  
information and said means for combining said first scrambled  
signal component and said second descrambled signal to produce  
said output signal being included in an IC mounted in said smart  
30 card; and

said first and second terminals being positioned on a  
surface of said smart card.

9. The smart card of claim 8 further comprising a third terminal positioned on said surface of said smart card for receiving a timing signal;

5       said means for producing said first and second descrambled signals being responsive to said timing signal for processing said input signal at a first data rate to produce said output signal at said first data rate.

10       10. The smart card of claim 9 wherein said first data rate exceeds 10 mega-Hertz.

15       11. The smart card of claim 9 wherein said means for producing said control information processes said first descrambled signal at a second data rate for producing said control information.

12. The smart card of claim 11 wherein said first data rate is greater than said second data rate.

20       13. The smart card of claim 12 further comprising a frequency divider coupled to receive said timing signal for producing a clock signal at a frequency related to said second data rate; said means for producing said control information being responsive to said clock signal for producing said control  
25       information.

14. The smart card of claim 5 wherein  
30       said first scrambled signal component comprises entitlement management information for a pay-for-access service; and

      said second scrambled signal component comprises data provided by said pay-for-access service.

35       15. The smart card of claim 14 wherein said pay-for-access service comprises a pay-TV service; said entitlement

management information comprises television programming entitlement information; and said data provided by said pay-for-access-service comprises television program data.

5           16. The smart card of claim 9 wherein said first, second and third terminals being included in a plurality of terminals arranged on said surface of said smart card in accordance with ISO standard 7816-2.

10           17. The smart card of claim 16 wherein said smart card exhibits a mechanical characteristic in accordance with ISO standard 7816-1.

1/8

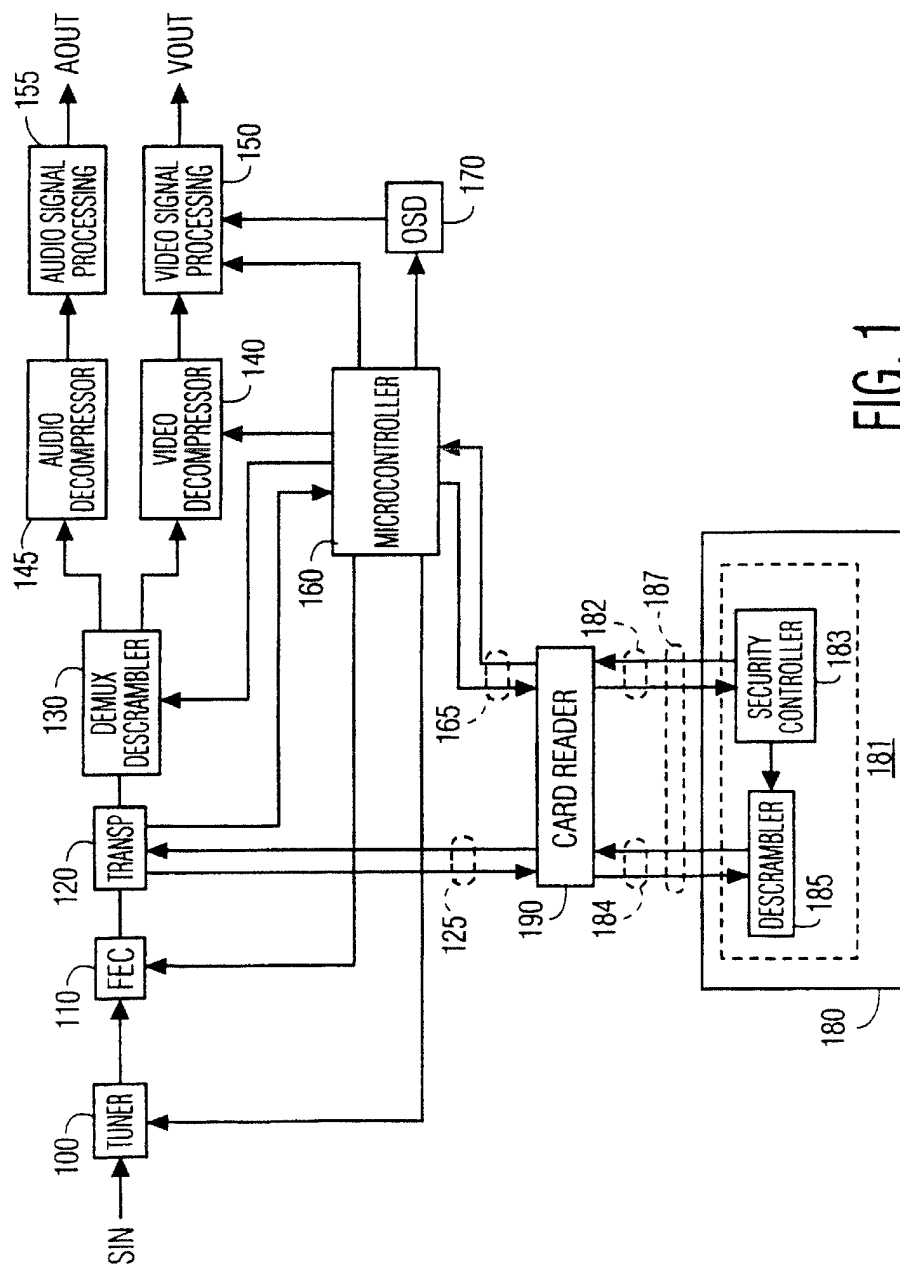


FIG. 1

SUBSTITUTE SHEET (RULE 26)

2/8

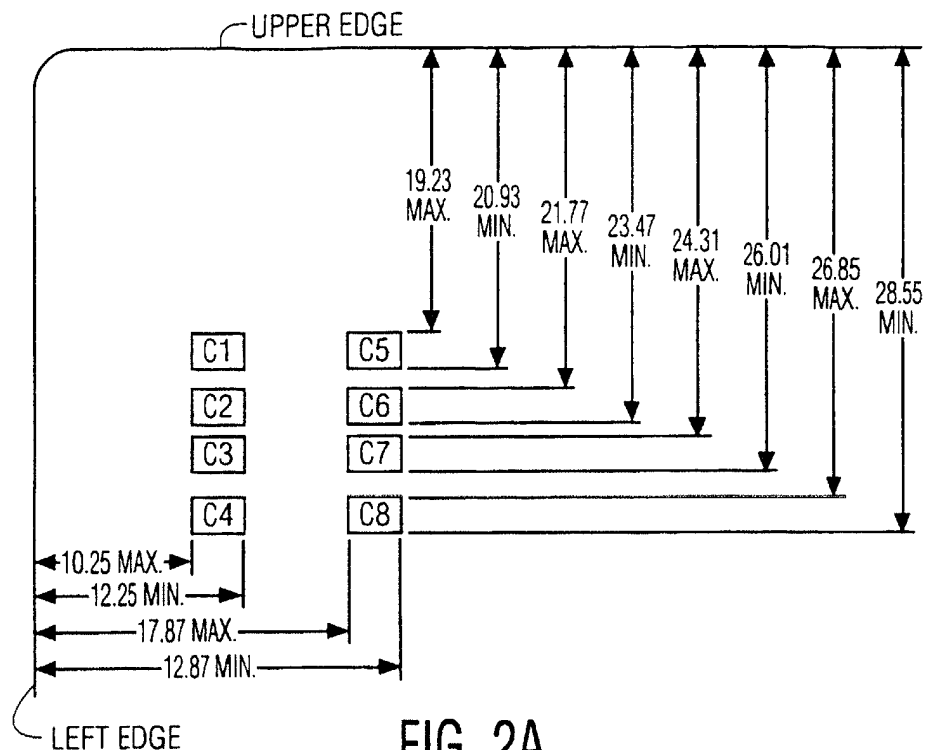


FIG. 2A

CONTACT NO.	ASSIGNMENT	CONTACT NO.	ASSIGNMENT
C1	VCC (SUPPLY VOLTAGE)	C5	GND (GROUND)
C2	RST (RESET SIGNAL)	C6	VPP (PROGRAMMING VOLTAGE)
C3	CLK (CLOCK SIGNAL)	C7	I/O (DATA INPUT/OUTPUT)
C4	RESERVED TO ISO/IEC JTC 1/SC 17 FOR FUTURE USE	C8	RESERVED TO ISO/IEC JTC 1/SC 17 FOR FUTURE USE

FIG. 2B

SUBSTITUTE SHEET (RULE 26)

3/8

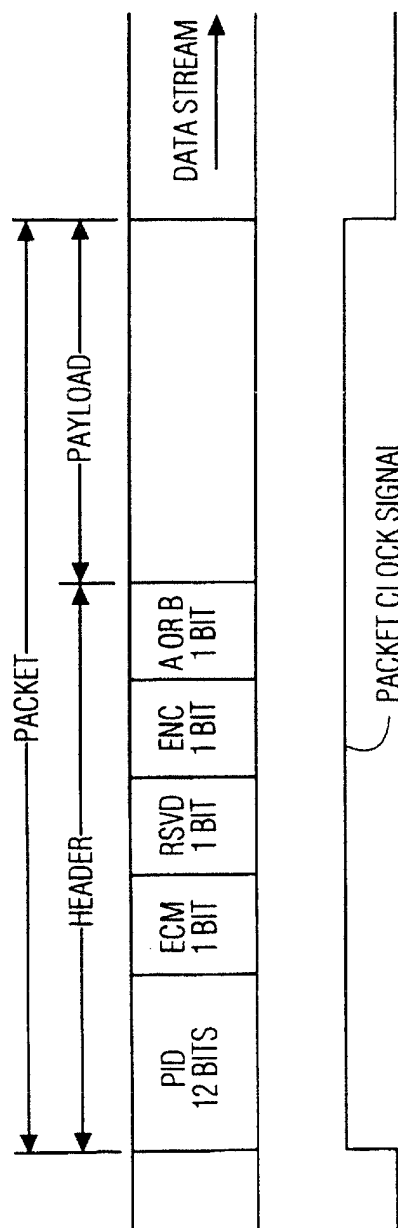


FIG. 3

SUBSTITUTE SHEET (RULE 26)



4/8

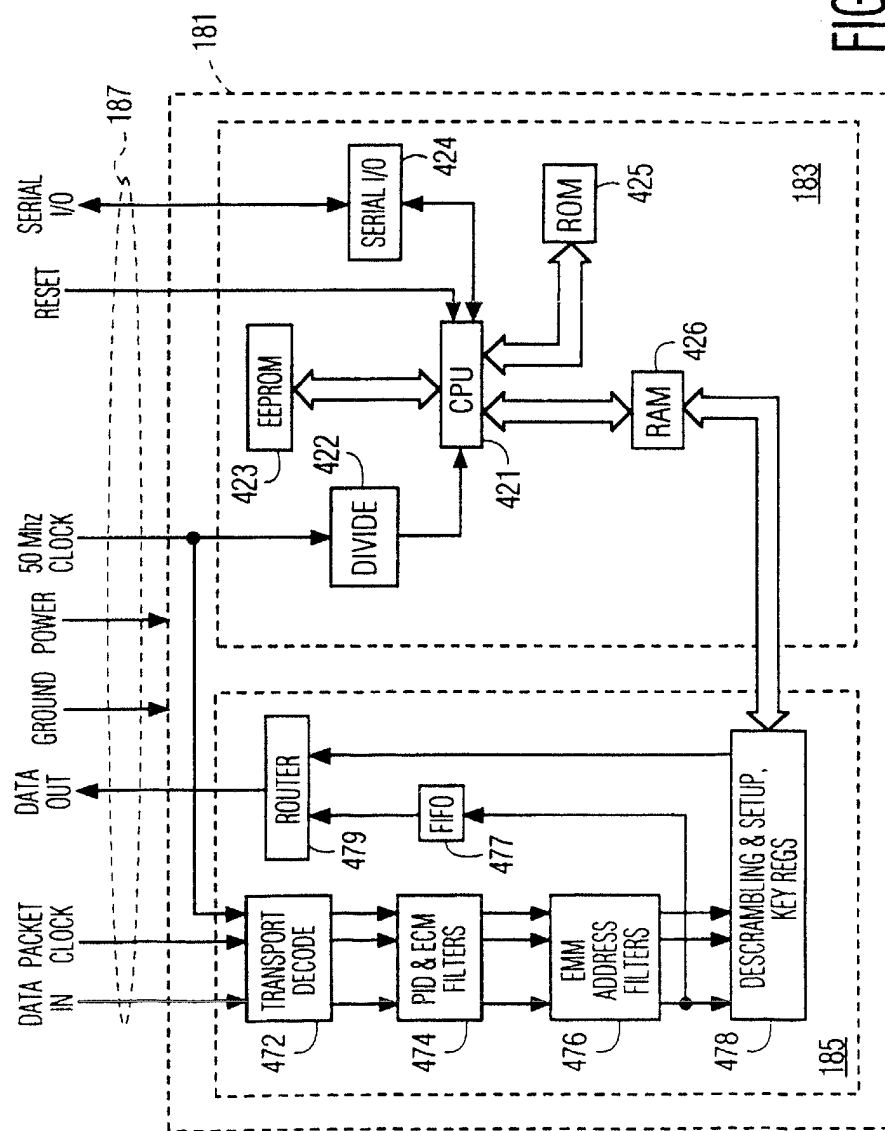
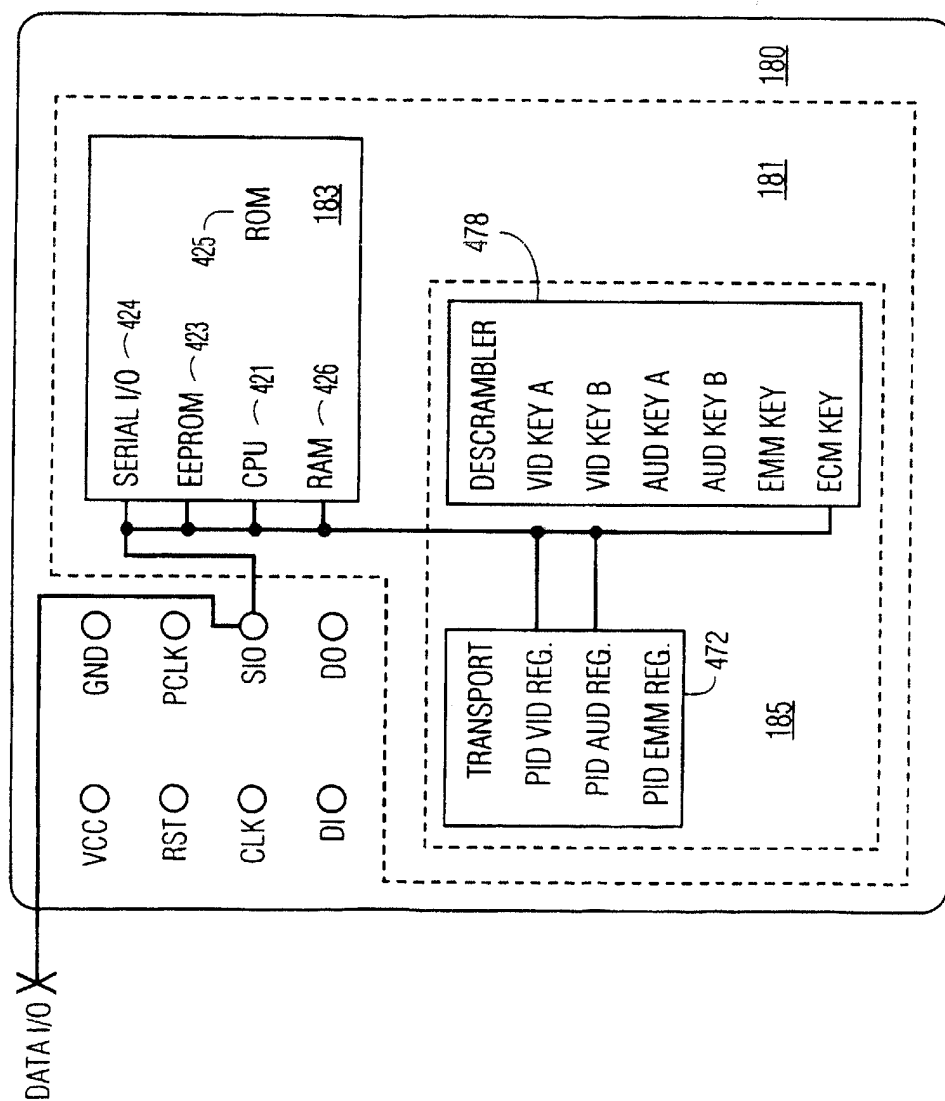


FIG. 4

SUBSTITUTE SHEET (RULE 26)

5/8

FIG. 5



SUBSTITUTE SHEET (RULE 26)

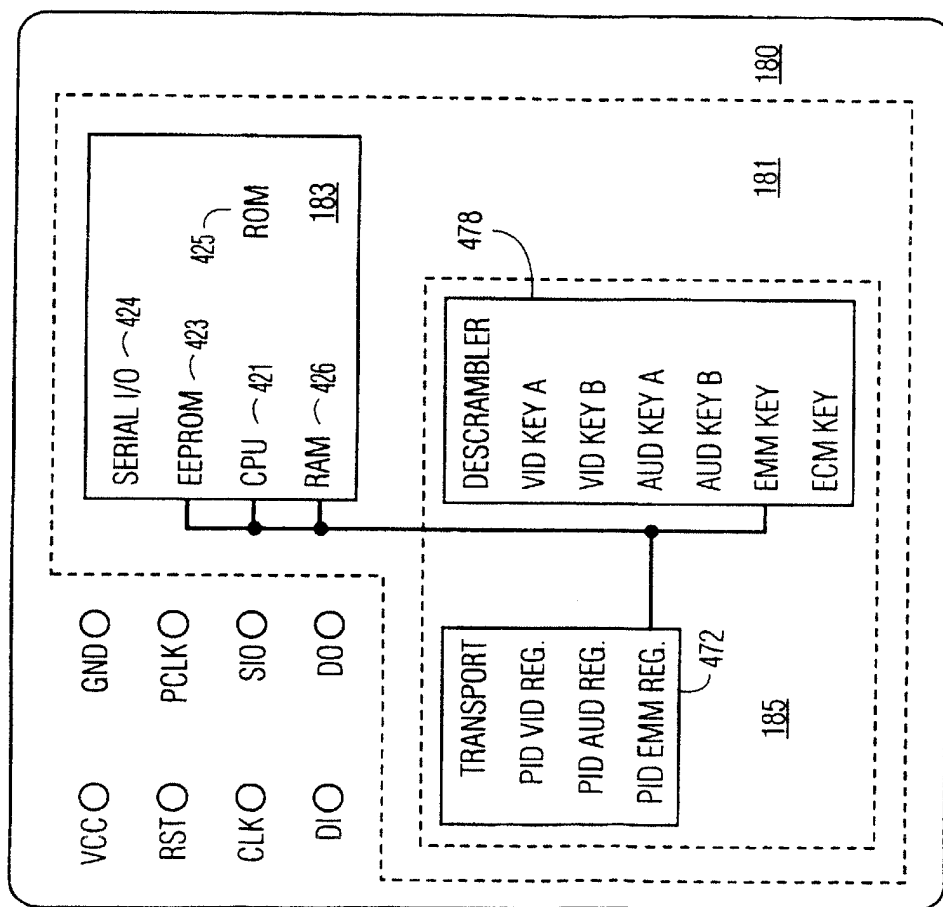
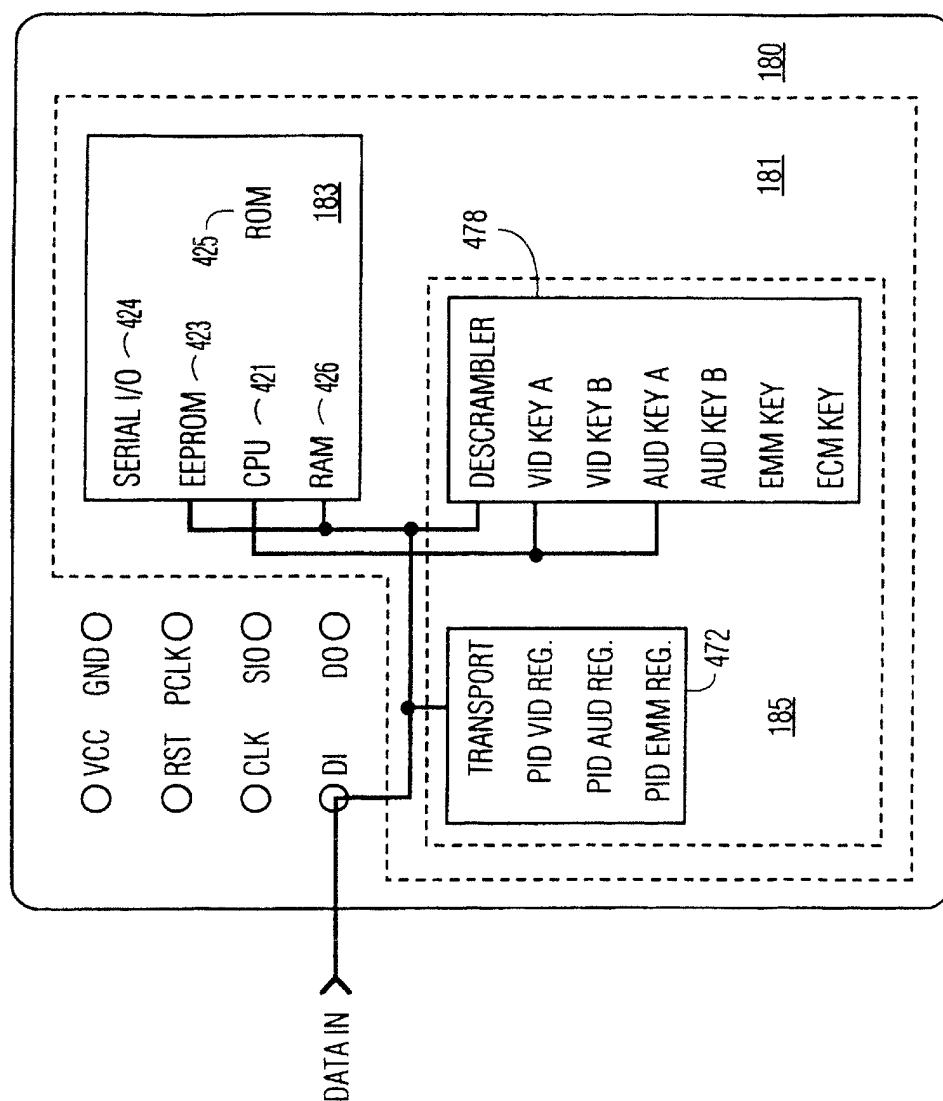


FIG. 6

7/8

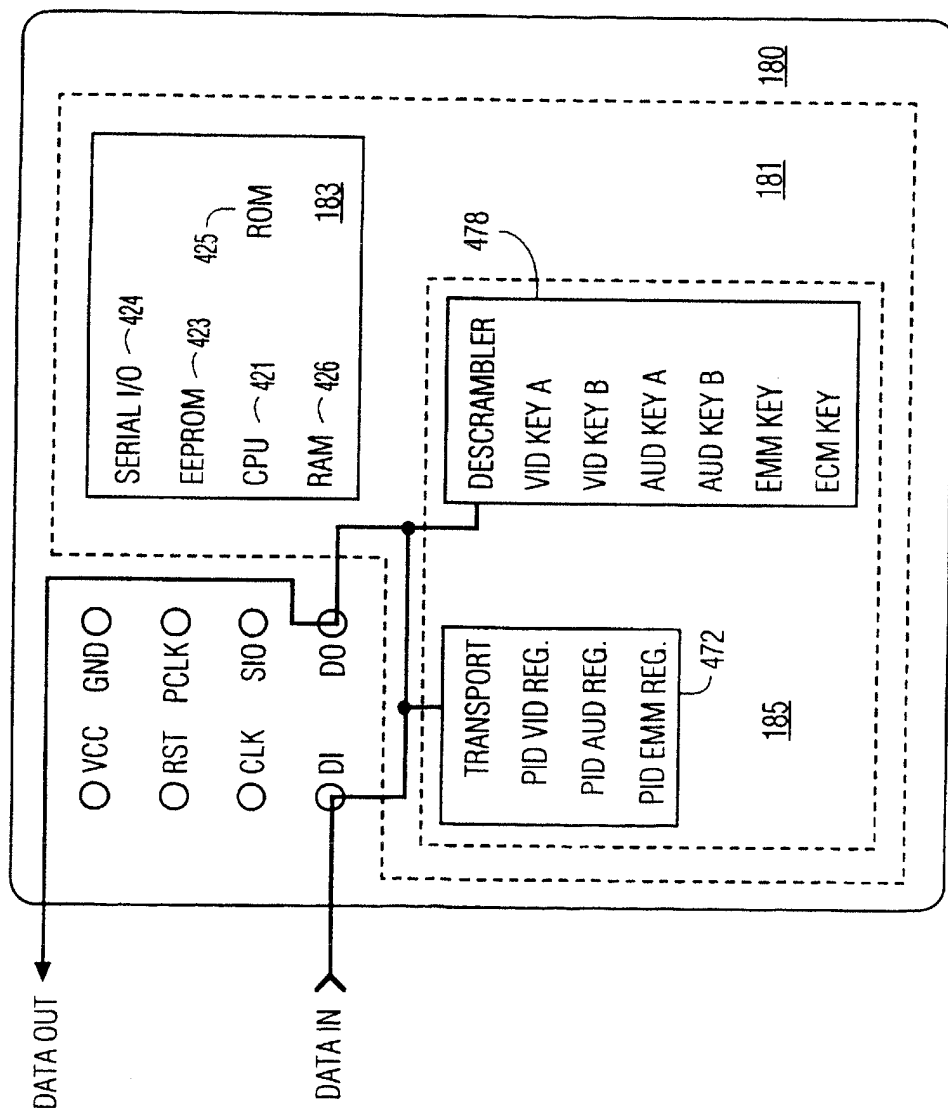
FIG. 7



SUBSTITUTE SHEET (RULE 26)

8/8

FIG. 8



SUBSTITUTE SHEET (RULE 26)

# INTERNATIONAL SEARCH REPORT

International Application No  
PCT/US 95/09953

A. CLASSIFICATION OF SUBJECT MATTER  
IPC 6 H04N7/167 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 G07F H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP, A, 0 428 252 (NEWS DATA SECURITY PRODUCTS) 22 May 1991 see abstract; claims; figures 1-3 ---	1, 5, 7, 8, 14, 15
Y	US, A, 4 993 066 (H.H. JENKINS) 12 February 1991 see the whole document ---	1, 5, 7, 8, 14, 15
A	EP, A, 0 588 184 (THOMSON CONSUMER ELECTRONICS) 23 March 1994 ---	
A	EP, A, 0 585 833 (NOKIA TECHNOLOGY) 9 March 1994 -----	

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

### \* Special categories of cited documents:

- \*A\* document defining the general state of the art which is not considered to be of particular relevance
- \*E\* earlier document but published on or after the international filing date
- \*L\* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- \*O\* document referring to an oral disclosure, use, exhibition or other means
- \*P\* document published prior to the international filing date but later than the priority date claimed

- \*T\* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- \*X\* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- \*Y\* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- \*G\* document member of the same patent family

Date of the actual completion of the international search

29 November 1995

Date of mailing of the international search report

21. 12. 95

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+ 31-70) 340-3016

Authorized officer

David, J

# INTERNATIONAL SEARCH REPORT

(information on patent family members)

International Application No

PCT/US 95/09953

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP-A-0428252	22-05-91	AU-B- 6230690 CA-A- 2025585 JP-A- 3210843	23-05-91 15-05-91 13-09-91
US-A-4993066	12-02-91	NONE	
EP-A-0588184	23-03-94	AU-B- 4615693 JP-A- 6197341 US-A- 5461675	24-03-94 15-07-94 24-10-95
EP-A-0585833	09-03-94	FI-A- 923980	05-03-94

Form PCT ISA 210 (patent family annex) (July 1992)

DISPOSITIFS POUR MASQUER LES OPERATIONS EFFECTUEES DANS  
UNE CARTE A MICROPROCESSEUR

L'invention concerne les cartes à microprocesseur et, dans de telles cartes, différents dispositifs pour masquer les opérations effectuées dans la carte dans le but d'améliorer la sécurité contre les intrusions frauduleuses.

Les cartes à puces se divisent en plusieurs catégories, à savoir :

- les cartes à simple mémoire,
- les cartes à mémoire dite carte intelligente, et
- les cartes à microprocesseur.

Une carte à simple mémoire permet d'effectuer des opérations de lecture et d'écriture dans la zone de mémoire morte électriquement effaçable de façon libre. Une telle carte est d'un faible coût mais elle ne présente pas une sécurité suffisante de sorte qu'elle est de moins en moins utilisée.

Une carte à mémoire intelligente améliore notamment la sécurité des opérations de lecture/écriture en les autorisant seulement lorsque certaines conditions réalisées sous forme câblée sont remplies.

Une carte de la troisième catégorie contient un microprocesseur capable d'exécuter des programmes enregistrés dans une mémoire et d'effectuer ainsi des calculs avec des données secrètes inaccessibles au monde extérieur à la carte. Ainsi, une clé enregistrée dans la mémoire peut servir à valider une transaction électronique telle qu'un achat ou une ouverture de porte sans avoir à être manipulée à l'extérieur de la carte.



Malheureusement, certains microprocesseurs présentent des consommations de courant qui dépendent des calculs effectués à l'intérieur de la carte. Ainsi, un calcul cryptographique comprenant une arborescence de calcul qui dépend des chiffres de la clé utilisée aura différentes empreintes de consommation de courant selon la valeur de la clé utilisée. Il en résulte qu'un fraudeur pourrait corrélérer l'empreinte de consommation de courant de la clé utilisée et ainsi remonter à la valeur de la clé.

Pour empêcher cette corrélation, une contre-mesure courante consiste à programmer l'algorithme cryptographique d'une manière telle que quelle que soit la valeur de la clé, l'algorithme passera toujours les mêmes étapes de calcul.

De nombreux algorithmes dits "orientés octets" se prêtent bien à ce mode de programme mais d'autres posent quelques problèmes techniques qui ne sont surmontables qu'au prix de performances calculatoires moins optimales.

La présente invention a donc pour but de mettre en oeuvre dans les cartes à microprocesseur des dispositifs pour masquer les opérations effectuées tout en permettant au programmeur le libre-choix des règles de programmation, qu'elles soient du type "orientées octets" ou non.

Ce but est atteint en modifiant ou brouillant la consommation de la carte de manière que son empreinte soit indépendante des calculs effectués.

Cette modification ou ce brouillage de l'empreinte peut être obtenue en ajoutant dans la carte un dispositif qui modifie la consommation de courant.

Dans un premier exemple de réalisation, ce dispositif consomme de la puissance électrique de

manière irrégulière ou aléatoire qui s'ajoute à celle de la consommation normale.

Dans un deuxième exemple de réalisation, ce dispositif réalise une consommation moyenne en  
5 réalisant, par exemple, une intégration du courant consommé.

Dans un troisième exemple de réalisation, ce dispositif déclenche le circuit de programmation ou d'effacement de la mémoire du microprocesseur qui  
10 consomme de la puissance de manière chaotique, puissance qui masque la consommation due aux opérations effectuées par le microprocesseur pendant la programmation ou l'effacement de la mémoire.

D'autres caractéristiques et avantages de la  
15 présente invention effectueront à la lecture de la description suivante d'exemples particuliers de réalisation, ladite description étant faite en relation avec les dessins joints dans lesquels :

- la figure 1 est un schéma fonctionnel d'un  
20 premier exemple de réalisation de l'invention,

- la figure 2 est un schéma fonctionnel d'un deuxième exemple de réalisation de l'invention, et

- la figure 3 est un schéma fonctionnel d'un troisième exemple de réalisation de l'invention.

25 Sur les figures qui montrent chacune schématiquement différents moyens pour réaliser l'invention, la puce électronique 10 contenant le microprocesseur de la carte comprend une unité centrale 12 et au moins une mémoire 14, par exemple du type  
30 connu sous l'acronyme anglo-saxon EEPROM FOR ELECTRICALLY ERASABLE PROGRAMMABLE READ ONLY MEMORY. Cette puce électronique présente plusieurs bornes d'entrée et/ou de sortie 16<sub>1</sub> à 16<sub>8</sub> dont l'une d'entre elles référencée 16<sub>1</sub> est connectée à un circuit

d'alimentation électrique 18 de tension  $V_{CC}$  tandis que celle référencée 16<sub>5</sub> est connectée à la masse.

Le circuit d'alimentation 18 alimente les différents éléments de la puce électronique 10 avec un courant  $I_{out}$  et, notamment, la mémoire 14 et l'unité centrale 12. Ce courant  $I_{out}$  varie en fonction des opérations effectuées par l'unité centrale et la mémoire et reflètent donc les calculs cryptographiques, ce qui pourrait permettre d'en déterminer la clé.

Pour que ce courant  $I_{out}$  ne reflète plus les opérations effectuées, l'invention propose de le modifier par un dispositif 20 ou 30, disposé dans la puce 10 et connecté, par exemple, sur la borne d'entrée 16<sub>1</sub>.

L'invention propose de modifier le courant de deux manières différentes. Une première en faisant en sorte que le dispositif 20 (figure 1) consomme du courant de manière aléatoire ou tout au moins irrégulière, consommation supplémentaire aléatoire qui s'ajoutant à la consommation normale de courant  $I_{in}$  rend aléatoire la valeur  $I_{out}$ .

La deuxième manière consiste à moyenner la valeur de  $I_{in}$ , ce qui ne permet pas de détecter les variations de  $I_{in}$  dues aux opérations effectuées.

Dans le premier cas, le dispositif 20 peut être réalisé à l'aide de résistances 30, en fait des transistors, qui sont alimentées ou non selon les signaux aléatoires fournis par un générateur 28. Les courants circulant dans les résistances alimentées augmentent, modifiant la valeur du courant total et masquant le courant dû aux calculs cryptographiques.

Dans le deuxième cas, la moyenne du courant  $I_{in}$  est obtenue par un intégrateur qui "lisse" les variations du courant  $I_{in}$  de manière à les effacer.

Selon l'invention, plusieurs dispositifs 20 ou 30, référencés 20<sub>1</sub> et 30<sub>1</sub> peuvent être connectés à différents endroits de la puce électronique, par exemple, sur le conducteur d'alimentation de l'unité centrale (référence 22). En outre, ces dispositifs 20, 20<sub>1</sub>, 30 et 30<sub>1</sub> peuvent être connectés ou non selon que les opérations doivent être sécurisées ou non, les connexions s'effectueront sous la commande de signaux fournis par l'unité centrale 12 (traits discontinus).

L'invention propose une troisième manière de brouiller la valeur de  $I_{out}$  en effectuant des opérations à sécuriser, telles que des calculs cryptographiques, pendant certaines phases des opérations de programmation ou d'effacement de la mémoire 14, ces opérations étant sur la commande de l'unité centrale 12.

Cette troisième manière repose sur l'utilisation d'une mémoire 14 de type EEPROM qui a la capacité d'auto-écriture.

Dans un mode habituel de fonctionnement, le microprocesseur met en marche un circuit de programmation 24 de la mémoire 14 selon les étapes suivantes :

- 1 - mise en marche de la pompe de charge,
- 25 2 - présentation sur le bus de données de la dernière à écrire,
- 3 - présentation sur le bus d'adresse de l'adresse écriture,
- 4 - mise en marche de la programmation,
- 30 5 - attente d'un délai de programmation,
- 6 - arrêt de la programmation,
- 7 - arrêt de la pompe de charge.

La programmation d'une cellule EEPROM nécessitant d'injecter des charges électriques dans la cellule

programmée, les étapes 4, 5 et 6 s'accompagnent d'une sur-consommation de courant d'apparence chaotique qui dépend essentiellement de la valeur de  $V_{cc}$ , de l'adresse, de la valeur programmée et de la température du composant.

Afin de masquer l'empreinte de consommation de courant d'un calcul cryptographique par exemple, l'invention propose d'utiliser la consommation chaotique des étapes 4, 5 et 6 en réalisant le calcul cryptographique pendant l'étape 5 d'une durée de quelques millisecondes.

Pour ce faire, le calcul cryptographique s'effectue selon les étapes suivantes :

- 1 - mise en marche de la pompe de charge,
- 2 - présentation sur le bus de données d'une donnée aléatoire,
- 3 - présentation sur le bus d'adresse d'une adresse écrite,
- 4 - mise en marche de la programmation,
- 5 - effectuer le calcul cryptographique,
- 6 - arrêt de la programmation,
- 7 - arrêt de la pompe à charge.

Par ces étapes, l'empreinte de la consommation de courant due au calcul cryptographique de l'étape 5 est masquée par l'écriture de la donnée aléatoire dans une partie déterminée 26 de la mémoire EEPROM réservée à cette fonction.

Au lieu d'un calcul cryptographique, l'étape 5 peut consister en toute opération à sécuriser vis-à-vis de l'extérieur.

Par ailleurs, au lieu de faire ces opérations à sécuriser lors d'une écriture dans la mémoire 14, elles peuvent être faites lors d'un effacement de la mémoire 14.

## REVENDEICATIONS

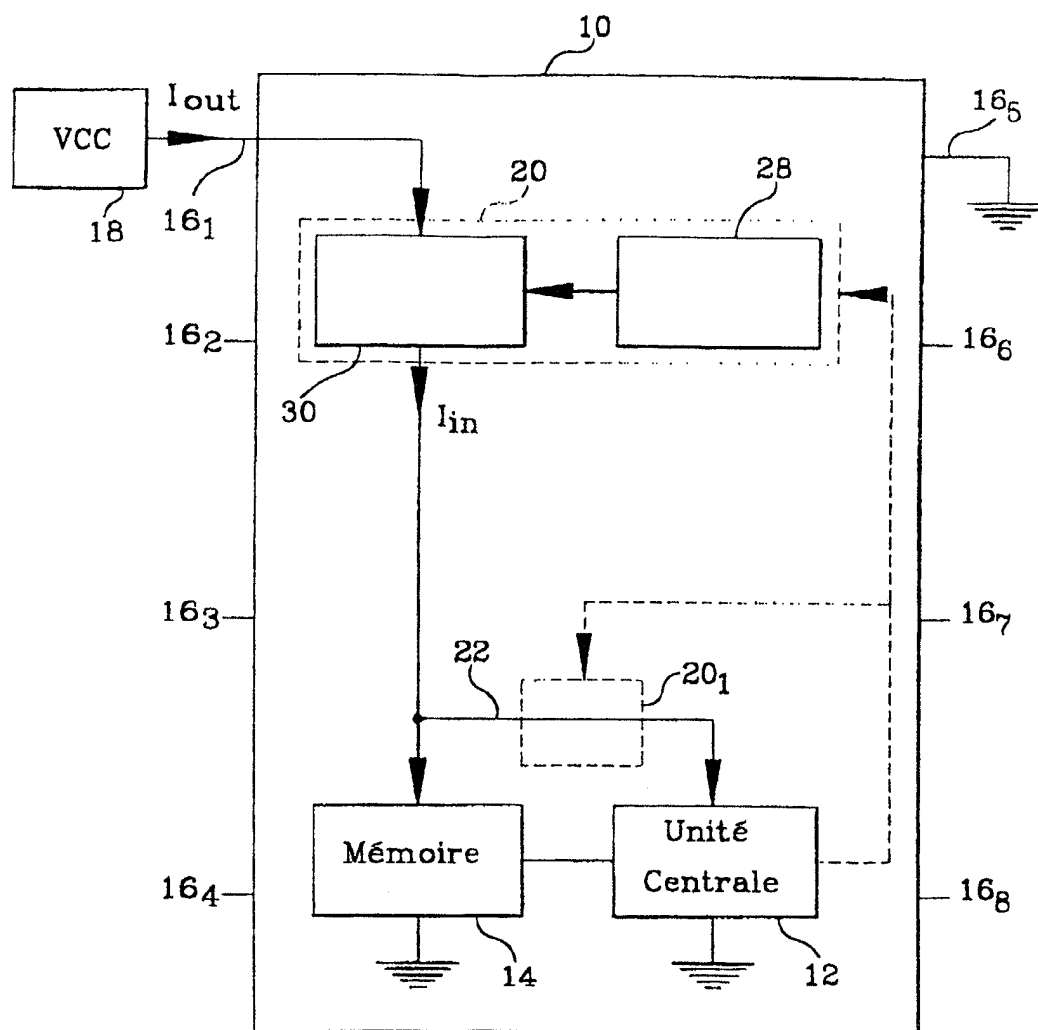
- 1 - Dispositif pour masquer les opérations effectuées par un composant destiné à être intégré à une carte à puce, caractérisé en ce qu'il comprend au moins un moyen (20, 30, 28, 26) pour modifier la consommation de courant dudit composant lors de la réalisation desdites opérations.
- 2 - Dispositif selon la revendication 1, caractérisé en ce que le moyen pour modifier la consommation de courant comprend au moins un circuit intégrateur (30) du courant du composant de manière à moyenner les variations de ce courant au cours du temps.
- 3 - Dispositif selon la revendication 1, caractérisé en ce que le moyen pour modifier la consommation de courant comprend au moins un générateur (28) de signaux aléatoires et une batterie de résistances (20) dont l'alimentation de chacune des résistances est commandée par les signaux aléatoires.
- 4 - Dispositif selon la revendication 1, caractérisé en qu'il comprend une pluralité de moyens (20, 20<sub>1</sub>, 30, 30<sub>1</sub>) pour modifier la consommation de courant.
- 5 - Dispositif selon la revendication 1, caractérisé en ce que le moyen pour modifier la consommation de courant du composant dans le cas d'une mémoire (14) du type EEPROM, consiste à effectuer simultanément:
  - une opération d'écriture ou d'effacement de la mémoire (14) dite de masquage, et
  - une opération du microprocesseur.
- 6 - Dispositif selon la revendication 5, caractérisé en ce que, pour mettre en oeuvre une opération d'écriture de masquage, la mémoire (14) comprend une partie (26) dédiée à l'enregistrement d'une donnée aléatoire.
- 7 - Dispositif selon l'une des revendications 1 à 5, caractérisé en ce que la mise en route de chacun des moyens de modification de la consommation de courant est commandée par le microprocesseur (12) de manière à être mis en route pour les seules opérations à sécuriser.
- 8 - Dispositif selon la revendication 5, caractérisé en ce que le microprocesseur (12) réalise au moins le calcul cryptographique selon les étapes suivantes:
  - mise en marche de la pompe de charge,
  - présentation sur le bus de données d'une donnée aléatoire,
  - présentation sur le bus d'adresse d'une adresse écriture,
  - mise en marche de la programmation,
  - effectuer le calcul cryptographique,
  - arrêt de la programmation,
  - arrêt de la pompe de charge,de manière à masquer l'empreinte de la consommation de courant occasionnée par ledit calcul cryptographique.

8

9 - Procédé pour masquer les opérations effectuées par un composant, caractérisé en ce qu'il comporte les étapes suivantes:

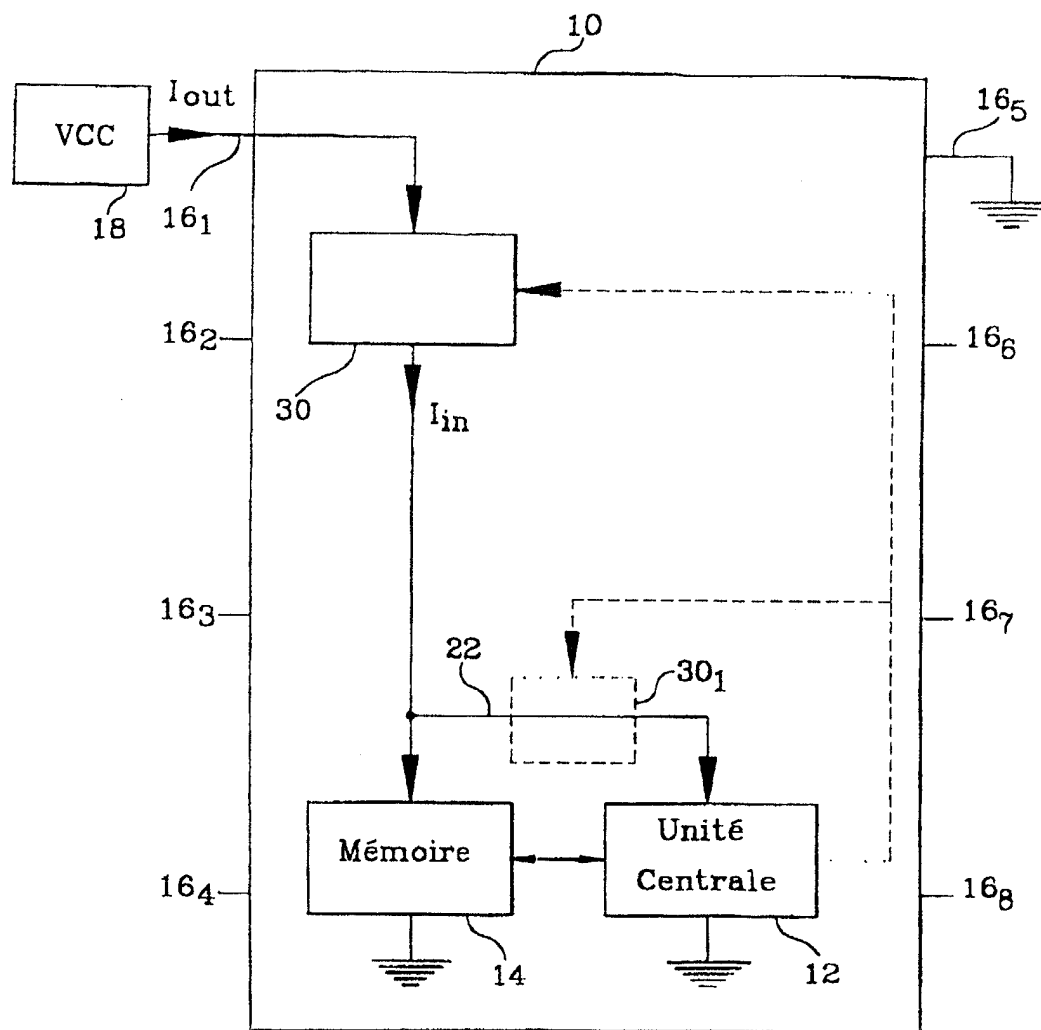
- mise en marche de la pompe de charge,
- présentation sur le bus de données d'une donnée aléatoire,
- présentation sur le bus d'adresse d'une adresse écriture,
- mise en marche de la programmation,
- effectuer le calcul cryptographique,
- arrêt de la programmation,
- arrêt de la pompe de charge.

1/3

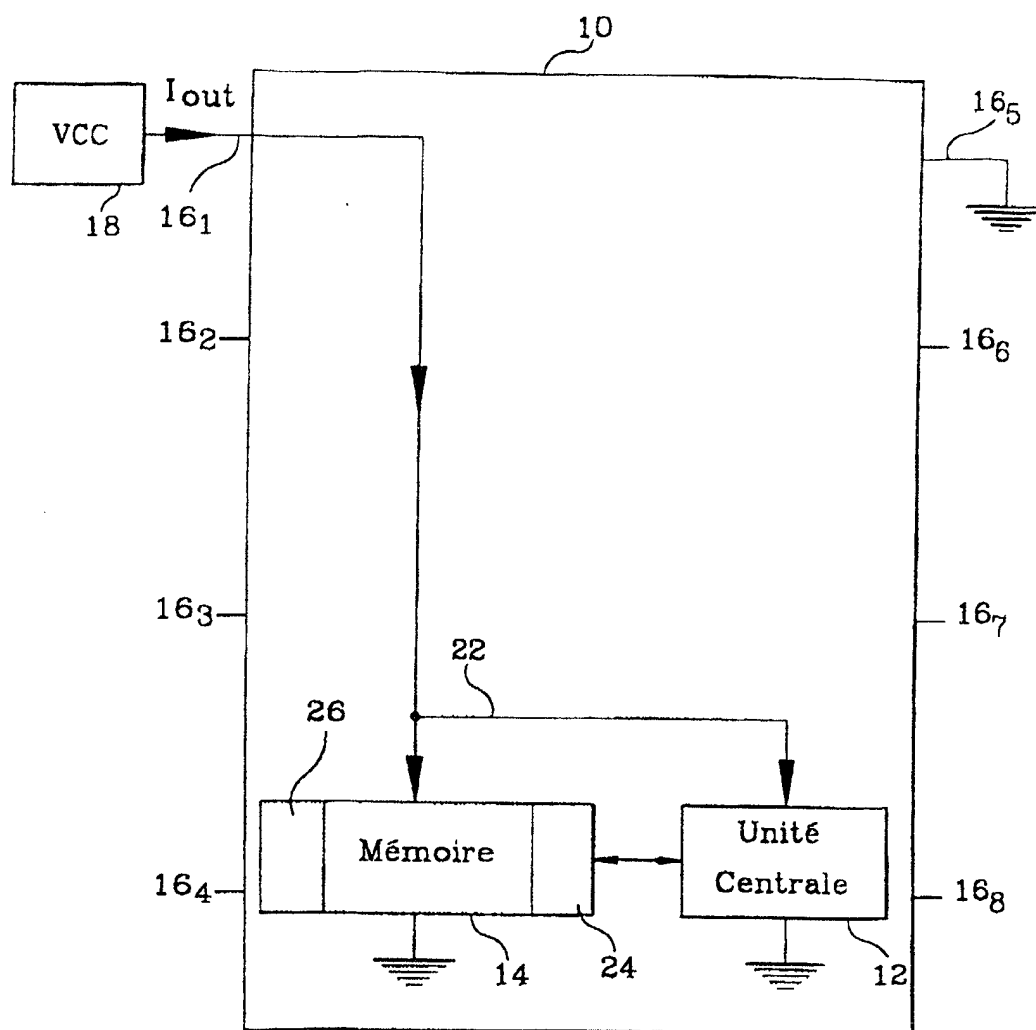
**FIG.1**



2/3

**FIG.2**

3/3

**FIG.3**

# INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 99/00583

A. CLASSIFICATION OF SUBJECT MATTER  
IPC 6 G06K19/073

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 G07F G06K G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 4 295 041 A (UGON MICHEL) 13 October 1981 see abstract; claim 1; figures 1,2 see column 1, line 61 - column 2, line 21 ---	1,5,7
X	US 4 932 053 A (FRUHAUF SERGE ET AL) 5 June 1990 see abstract; figure 4 see column 2, line 29-59 see column 3, line 26 - column 4, line 21 ---	1,3,4,7
Y		6
X	US 4 813 024 A (LISIMAQUE GILLES ET AL) 14 March 1989 see column 2, line 8-31 see column 3, line 63 - column 4, line 13 see column 6, line 18-22 ---	1,5,7
Y		6,8,9
	--- -/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

15 June 1999

Date of mailing of the international search report

21/06/1999

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Cardigos dos Reis, F

# INTERNATIONAL SEARCH REPORT

International Application No  
PCT/FR 99/00583

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	<p>WO 96 06504 A (CHANEY JOHN WILLIAM ; THOMSON CONSUMER ELECTRONICS (US)) 29 February 1996 see page 1, line 5-20 see page 2, line 3-10 see page 13, line 8-20 see page 22, line 9-18 -----</p>	8,9

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 99/00583

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 4295041	A	13-10-1981	FR 2401459 A	23-03-1979
			FR 2460506 A	23-01-1981
			CH 631561 A	13-08-1982
			DE 2837201 A	01-03-1979
			DE 2858818 C	29-08-1996
			DE 2858819 C	09-03-1995
			DE 2858829 C	28-11-1996
			GB 2004394 A, B	28-03-1979
			JP 54046447 A	12-04-1979
			JP 62056556 B	26-11-1987
			JP 2506061 B	12-06-1996
			JP 7093501 A	07-04-1995
			JP 1826230 C	28-02-1994
			JP 2210590 A	21-08-1990
			JP 3050314 B	01-08-1991
			JP 1556417 C	23-04-1990
			JP 62070993 A	01-04-1987
			JP 63025393 B	25-05-1988
			JP 2097860 C	02-10-1996
			JP 5217034 A	27-08-1993
			JP 8007780 B	29-01-1996
			US 4211919 A	08-07-1980
			DE 3025044 A	27-05-1981
			JP 56038651 A	13-04-1981
			JP 2547379 B	23-10-1996
			JP 8110937 A	30-04-1996
			JP 1152589 A	15-06-1989
			JP 2043222 B	27-09-1990
			JP 2547368 B	23-10-1996
			JP 5274499 A	22-10-1993
US 4932053	A	05-06-1990	FR 2638869 A	11-05-1990
			EP 0368727 A	16-05-1990
			JP 2199561 A	07-08-1990
			JP 2813663 B	22-10-1998
US 4813024	A	14-03-1989	FR 2600183 A	18-12-1987
			DE 3777701 A	30-04-1992
			EP 0251853 A	07-01-1988
			JP 63080351 A	11-04-1988
WO 9606504	A	29-02-1996	AU 3238595 A	22-03-1996
			AU 701593 B	04-02-1999
			AU 3239495 A	14-03-1996
			BR 9508621 A	30-09-1997
			BR 9508622 A	19-05-1998
			CA 2196406 A	07-03-1996
			CA 2196407 A	29-02-1996
			CN 1158202 A	27-08-1997
			CN 1158203 A	27-08-1997
			EP 0878088 A	18-11-1998
			EP 0782807 A	09-07-1997
			FI 970677 A	18-02-1997
			JP 10506507 T	23-06-1998
			JP 10505720 T	02-06-1998
			PL 318647 A	07-07-1997
			WO 9607267 A	07-03-1996

PCT/FR 99/00583

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 6 G07F G06K G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
-------------	--	-------------------------------

1,5,7

1,3,4,7

6

- / - -

☒ Les documents de familles de brevets sont indiqués en annexe

"&" document qui fait partie de la même famille de brevets

Date d'expédition du présent rapport de recherche internationale

21/06/1999

Fonctionnaire autorisé

Cardigos dos Reis, F

# RAPPORT DE RECHERCHE INTERNATIONALE

Der. de internationale No  
PCT/FR 99/00583

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS		
Categorie	Identification des documents cites, avec, le cas echeant, l'indication des passages pertinents	no. des revendications visees
X	US 4 813 024 A (LISIMAQUE GILLES ET AL) 14 mars 1989	1,5,7
Y	voir colonne 2, ligne 8-31 voir colonne 3, ligne 63 - colonne 4, ligne 13 voir colonne 6, ligne 18-22	6,8,9
Y	WO 96 06504 A (CHANEY JOHN WILLIAM ; THOMSON CONSUMER ELECTRONICS (US)) 29 février 1996 voir page 1, ligne 5-20 voir page 2, ligne 3-10 voir page 13, ligne 8-20 voir page 22, ligne 9-18	8,9

# RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Den...de Internationale No

PCT/FR 99/00583

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 4295041 A	13-10-1981	FR 2401459 A	23-03-1979
		FR 2460506 A	23-01-1981
		CH 631561 A	13-08-1982
		DE 2837201 A	01-03-1979
		DE 2858818 C	29-08-1996
		DE 2858819 C	09-03-1995
		DE 2858829 C	28-11-1996
		GB 2004394 A,B	28-03-1979
		JP 54046447 A	12-04-1979
		JP 62056556 B	26-11-1987
		JP 2506061 B	12-06-1996
		JP 7093501 A	07-04-1995
		JP 1826230 C	28-02-1994
		JP 2210590 A	21-08-1990
		JP 3050314 B	01-08-1991
		JP 1556417 C	23-04-1990
		JP 62070993 A	01-04-1987
		JP 63025393 B	25-05-1988
		JP 2097860 C	02-10-1996
		JP 5217034 A	27-08-1993
		JP 8007780 B	29-01-1996
		US 4211919 A	08-07-1980
		DE 3025044 A	27-05-1981
		JP 56038651 A	13-04-1981
		JP 2547379 B	23-10-1996
		JP 8110937 A	30-04-1996
		JP 1152589 A	15-06-1989
		JP 2043222 B	27-09-1990
		JP 2547368 B	23-10-1996
		JP 5274499 A	22-10-1993
US 4932053 A	05-06-1990	FR 2638869 A	11-05-1990
		EP 0368727 A	16-05-1990
		JP 2199561 A	07-08-1990
		JP 2813663 B	22-10-1998
US 4813024 A	14-03-1989	FR 2600183 A	18-12-1987
		DE 3777701 A	30-04-1992
		EP 0251853 A	07-01-1988
		JP 63080351 A	11-04-1988
WO 9606504 A	29-02-1996	AU 3238595 A	22-03-1996
		AU 701593 B	04-02-1999
		AU 3239495 A	14-03-1996
		BR 9508621 A	30-09-1997
		BR 9508622 A	19-05-1998
		CA 2196406 A	07-03-1996
		CA 2196407 A	29-02-1996
		CN 1158202 A	27-08-1997
		CN 1158203 A	27-08-1997
		EP 0878088 A	18-11-1998
		EP 0782807 A	09-07-1997
		FI 970677 A	18-02-1997
		JP 10506507 T	23-06-1998
		JP 10505720 T	02-06-1998
		PL 318647 A	07-07-1997
		WO 9607267 A	07-03-1996